bitdefender

TOTAL SECURITY 2008

Manual do Utilizador

Copyright© 2008 BitDefender

BitDefender Total Security 2008

Manual do Utilizador

Publicado 2008.03.26

Copyright© 2008 BitDefender

Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, electrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de arquivo de informação, sem a permissão por escrito de um representante autorizado de BitDefender. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

Aviso e Renúncia. Este produto e a sua documentação estão protegidas por direitos de autor. A informação neste documento é apresentada numa base de "tal como é", sem qualquer garantia. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não serão responsabilizados por qualquer pessoa ou entidade com respeito a qualquer perda ou dano causado ou alegadamente causado directa ou indirectamente pela informação contida neste livro.

Este livro contém links para Websites de terceiras partes que não estão baixo controlo da BitDefender, e a BitDefender não é responsável pelo conteúdo de qualquer site acedido por link. Se aceder a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A BitDefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a BitDefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

Marcas Registadas. Nomes de Marcas Registadas poderão aparecer neste livro. Todas as marcas registadas ou não registadas neste documento são da exclusiva propriedade dos seus respectivos proprietários.

bitdefender

Índice

Licença e garantia ..... **ix**

Prefácio ..... **xiii**

1. Convenções Usadas neste Manual xiii
   1.1. Convenções Tipográficas xiii
   1.2. Avisos xiv
2. A estrutura do Manual xiv
3. Pedido de Comentários xv

Instalação ***1***

1. Instalação do BitDefender Total Security 2008 ..... **2**

1.1. Requisitos do Sistema 2
1.2. Passos da Instalação 3
1.3. Assistente Inicial de Instalação 5
1.3.1. Passo 1/6 - Registar o BitDefender Total Security 2008 6
1.3.2. Passo 2/6 - Criar uma conta BitDefender 7
1.3.3. Passo 3/6 - Saber mais acerca de RVTR (Relatório de Vírus em Tempo Real) 9
1.3.4. Passo 4/6 - Seleccionar as Tarefas a Serem Executadas 10
1.3.5. Passo 5/6 - Esperar que as Tarefas Terminem 11
1.3.6. Passo 6/6 - Ver Resumo 12
1.4. Upgrade (Mudança de versão) 12
1.5. Remover ou Reparar o BitDefender 13

Administração Básica ***15***

2. Introdução **16**

2.1. Ícone BitDefender na Área de Notificação 17
2.2. Barra de Actividade da Análise 18
2.3. Análise Manual BitDefender 19
2.4. Modo de Jogo 19
2.4.1. Usar o Modo de Jogo 20
2.4.2. Mudar a Hotkey do Modo de Jogo 20

3. Estado de Segurança **21**

3.1. Botão De Estado De Segurança 23
3.2. Botão de Estado do Controlo Parental 24
3.3. Botão de Estado TuneUp 24
3.4. Botão de Estado do Backup 25

4. Tarefas Rápidas **27**

4.1. Segurança 27

4.1.1. Actualizar o BitDefender ... 27
4.1.2. A analisar com BitDefender ... 29
4.2. Backup ... 34
4.2.1. Iniciar Assistente de Backup ... 34
4.2.2. Iniciar Assistente de Restauro ... 39
4.3. TuneUp ... 43
4.3.1. Desfragmentar Volumes de Discos Duros ... 44
4.3.2. Localizar Ficheiros Duplicados ... 47
4.3.3. Limpar Ficheiros da Internet ... 52
4.3.4. Apagar Ficheiros Permanentemente ... 55
4.3.5. Limpar o Registo ... 58
4.3.6. Recuperar Limpeza de Registo ... 62

5. Histórico ... 65

6. Registo ... 67
6.1. Passo 1/3 - Registar o BitDefender Total Security 2008 ... 67
6.2. Passo 2/3 - Criar uma conta BitDefender ... 68
6.3. Passo 3/3 - Registar o BitDefender Total Security 2008 ... 70

Administração de Segurança Avançada ... 71

7. Consola de Configuração ... 72
7.1. Configurações Gerais ... 73
7.1.1. Configurações Gerais ... 74
7.1.2. Configurações do Relatório de Vírus ... 75
7.1.3. Configurações de Administração ... 75

8. Antivírus ... 77
8.1. Análise No-acesso ... 77
8.1.1. Configurar Nível de Protecção ... 78
8.1.2. Personalizando Nível de Protecção ... 79
8.1.3. Desactivando a Protecção em Tempo-real ... 83
8.2. Análise A-pedido ... 83
8.2.1. Tarefas de Análise ... 85
8.2.2. Usando o Menú de Atalho ... 87
8.2.3. Criando Tarefas de Análise ... 88
8.2.4. Configurar Tarefas de Análise ... 88
8.2.5. Analisar objectos ... 99
8.2.6. Ver os Relatórios da Análise ... 106
8.3. Objectos a Excluir da Análise ... 108
8.3.1. Excluir Caminhos da Análise ... 110
8.3.2. Excluir Extensões da Análise ... 112
8.4. Àrea de Quarentena ... 115
8.4.1. Gerir Ficheiros em Quarentena ... 115
8.4.2. Configuração da Quarantena ... 116

9. Firewall 118
9.1. Compreender a Firewall 118
9.1.1. O que é um Perfil de Firewall? 119
9.1.2. O que São Zonas de Rede? 120
9.1.3. Operação da Firewall 121
9.2. Estado da Firewall 122
9.2.1. Configurar Nível de Protecção 124
9.3. Controlo de Tráfego 125
9.3.1. Adicionar Regras Automaticamente 125
9.3.2. Adicionar Regras Manualmente 126
9.3.3. Gerir Regras 131
9.3.4. Modificar Perfis 131
9.3.5. Reiniciar Perfis 133
9.4. Configuração Avançada 134
9.4.1. Configurações Filtro ICMP 135
9.4.2. Configuração Avançada da Firewall 137
9.5. Controlo de Ligação 138
9.6. Zonas de Rede 140
9.6.1. Adicionar Zonas 142

10. Antispam 144
10.1. Compreender o Antispam 144
10.1.1. Filtros Antispam 144
10.1.2. Operação Antispam 147
10.2. Estado do Antispam 148
10.2.1. Passo 1/2 - Definir o Nível de Tolerância 150
10.2.2. Passo 2/2 - Preencher a Lista de Endereços 151
10.3. Configurações de Antispam 155
10.3.1. Configurações de Antispam 156
10.3.2. Filtros Antispam Básicos 156
10.3.3. Filtros Antispam Avançados 157
10.4. Integração com Clientes de Mail 157
10.4.1. Barra de Ferramentas do Antispam 157
10.4.2. Assistente de Configuração Antispam 166

11. Controlo Privacidade 172
11.1. Estado do Controlo de Privacidade 172
11.1.1. Controlo Privacidade 173
11.1.2. Protecção Antiphishing 174
11.2. Configuração Avançada - Controlo de Identidade 175
11.2.1. Criar Regras de Identidade 177
11.2.2. Definir Excepções 179
11.2.3. Gerir Regras 180
11.3. Configuração Avançada - Controlo de registo 181
11.4. Configuração Avançada - Controlo de Cookies 183
11.4.1. Assistente de Configuração 185

11.5. Configuração Avançada - Controlo de Script 187
11.5.1. Assistente de Configuração 189
11.6. Info do Sistema 189
11.7. Barra de Ferramentas do Antiphishing 191

12. Controlo Parental 194
12.1. Proteger as Definições do Controlo Parental 194
12.2. Estado do Controlo Parental 195
12.2.1. Seleccionar Controlo de Protecção 196
12.2.2. Configurar Filtro Web Heurístico 197
12.3. Controlo Web 198
12.3.1. Assistente de Configuração 199
12.3.2. Especificar Excepções 200
12.3.3. Lista Negra Web BitDefender 201
12.4. Controlo de aplicações 201
12.4.1. Assistente de Configuração 202
12.5. Filtragem Palavra-chave 203
12.5.1. Assistente de Configuração 204
12.6. Temporizador Web 206

13. Actualização 208
13.1. Actualização Automática 209
13.1.1. Solicitar uma Actualização 210
13.1.2. Desactivar Actualização Automática 210
13.2. Definições de actualização 211
13.2.1. Configuração da Localização da Actualização 212
13.2.2. Configurar Actualização Automática 212
13.2.3. Configurar Actualização Manual 213
13.2.4. Configuração Avançada 213
13.2.5. Gerir Proxies 214

Administração de Backup Avançada 217

14. Administração de Backup Avançada 218
14.1. Barra de Menu 218
14.2. Barra de Navegação 220
14.2.1. Introdução 221
14.2.2. Gestor de Tarefa 222
14.2.3. Visualizar Log 246
14.2.4. Toolbox 250

CD de Emergência BitDefender 252

15. Geral 253
15.1. Requisitos do Sistema 253
15.2. Software incluído 254

16. Como Usar o CD de Emergência BitDefender 257
16.1. Iniciar o CD de Emergência BitDefender 257
16.2. Parar o CD de Emergência BitDefender 258
16.3. Como posso levar a cabo uma análise completa ao sistema? 259
16.4. Como posso actualizar o BitDefender através de um proxy? 260
16.5. Como posso salvar os meus dados? 261

Obter Ajuda 263

17. Suporte 264
17.1. BitDefender Knowledge Base 264
17.2. Pedir Ajuda 265
17.2.1. Vá até ao Self-Service Web 265
17.2.2. Abrir um ticket de suporte 265
17.3. Informação de Contacto 266
17.3.1. Endereços Web 266
17.3.2. Escritórios 266

Glossário 269

Licença e garantia

SE NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES NÃO INSTALE O SOFTWARE. AO SELECCIONAR "EU ACEITO", "OK", "CONTINUAR", "SIM" OU AO INSTALAR E USAR O SOFTWARE DE QUALQUER FORMA, ESTÁ A AFIRMAR QUE COMPREENDEU COMPLETAMENTE E ACEITOU OS TERMOS DE ESTE ACORDO.

Estes termos abrangem as Soluções e Serviços BitDefender para utilizadores individuais que lhe foram licenciadas, incluindo documentação relacionada, updates (actualizações da base de vírus) e upgrades (mudanças de versão) das aplicações que lhe foram entregues como parte da licença adquirida ou qualquer acordo de serviço tal como definido na documentação ou em qualquer cópia desses itens.

Este Acordo da Licença é um acordo legal entre você (seja um indivíduo ou representante legal) e a BITDEFENDER para uso do produto de software BITDEFENDER acima identificado, o qual inclui software de computador e serviços e poderá incluir meios associados, materiais impressos, e documentação "online" ou electrónica (daqui em diante designado por "BitDefender"), todos os quais estão protegidos pelos pelas leis internacionais dos direitos de autor e tratados internacionais. Ao instalar, copiar, ou usar de outra forma o BitDefender, estará a concordar com os termos deste acordo.

Se não concorda com os termos deste acordo, não instale ou use o BitDefender.

Licença BitDefender. O BitDefender está protegido pelas leis dos direitos de autor e pelos tratados internacionais sobre direitos de autor, como também por outras leis e tratados intelectuais de propriedade. O BitDefender é licenciado, não é vendido.

CONCESSÃO DE LICENÇA. Pela presente, a BITDEFENDER concede-lhe a si, e apenas a si a seguinte licença não-exclusiva, limitada, não-transmissível e passível de royaltie para utilizar o BitDefender.

SOFTWARE APLICAÇÃO. Pode instalar e usar BitDefender, em tantos computadores quantos os abrangidos pelo número total de licenças de utilizador. Pode fazer uma cópia adicional para efeitos de back-up (cópia de segurança).

LICENÇA DE UTILIZADOR DE COMPUTADOR INDIVIDUAL. Esta licença aplica-se ao software BitDefender que pode ser instalado num único computador que não providencie serviços de rede. O utilizador primário pode instalar este software num único computador e fazer uma cópia adicional num dispositivo distinto para efeitos de backup. O número de utilizadores primários permitidos corresponde ao número de utilizadores abrangidos pela licença.

TERMOS DE LICENÇA. A Licença aqui outorgada começa na data da aquisição do BitDefender e expira no final do período para o qual a licença foi adquirida.

EXPIRAÇÂO. O produto deixará de executar as suas funções imediatamente após a expiração da licença.

UPGRADES. Se o BitDefender estiver marcado como um upgrade (mudança de versão), tem de estar correctamente licenciado para usar um produto identificado pela BITDEFENDER como sendo elegível para o upgrade para poder usar o BitDefender. O BitDefender marcado como upgrade substitui e/ou suplementa o produto que forma as bases para a sua elegibilidade de upgrade. Pode utilizar o produto resultante do upgrade apenas nos termos deste Acordo de Licença. Se o BitDefender for um upgrade de um componente de um pacote de programas de software que licenciou como um único produto, o BitDefender pode ser usado e transferido apenas como uma parte desse único pacote de produtos, e não pode ser separado para uso por mais do que o número total de utilizadores licenciados. Os termos e condições desta licença substituem quaisquer acordos prévios que possam ter existido entre si e a BITDEFENDER com respeito ao produto original ou ao upgrade resultante.

DIREITOS DE AUTOR. Todos os direitos, títulos e interesses no e para o BitDefender e todos os direitos de autor em e no BitDefender (incluindo mas não limitado a qualquer imagem, fotografias, acessos, animações, vídeo, som, música, texto, e "applets" incorporadas no BitDefender), os materiais impressos que o acompanham, e quaisquer cópias do BitDefender são propriedade da BITDEFENDER. O BitDefender está protegido pelos direitos de autor e pelos tratados internacionais. Assim sendo, tem de tratar o BitDefender como qualquer outro material com direitos de autor. Não pode copiar os materiais impressos que acompanham o BitDefender. Tem de produzir e incluir todos os avisos de direitos de autor na sua forma original em todas as cópias criadas independentemente dos meios ou formas, nos quais o BitDefender existe. Não pode sub-licenciar, alugar, vender, fazer leasing ou partilhar a licença BitDefender. Não pode inverter a engenharia, recompilar, desmontar, criar trabalhos derivados, modificar, traduzir, ou fazer qualquer tentativa para descobrir a fonte do código do BitDefender.

GARANTIA LIMITADA. A BITDEFENDER garante que os meios, nos quais o BitDefender é distribuído, são livres de defeitos por um período de trinta dias desde a data de entrega do BitDefender a si. A única solução para uma quebra desta garantia será que a BITDEFENDER, em sua opção, poderá substituir o meio defeituoso após o recebimento do produto danificado, ou reembolsar-lhe o dinheiro que pagou pelo BitDefender. A BITDEFENDER não garante que o BitDefender não seja interrompido ou livre de erros, ou que os erros sejam corrigidos. A BITDEFENDER não garante que BitDefender vá de encontro às suas expectativas.

EXCEPTO TAL COMO EXPRESSAMENTE EXPOSTO NESTE ACORDO, BITDEFENDER RENUNCIA TODAS AS OUTRAS GARANTIAS, TANTO EXPRESSAS COMO IMPLÍCITAS, COM RESPEITO AOS PRODUTOS, MELHORIAS, MANUTENÇÃO OU SUPORTE RELACIONADOS COM ESTE ACORDO, OU QUAISQUER OUTROS MATERIAIS (TANGÍVEIS OU INTANGÍVEIS) OU SERVIÇOS FORNECIDOS POR ELE. A BITDEFENDER EXPRESSA AQUI A SUA RENÚNCIA A TODAS AS OUTRAS GARANTIAS, TANTO ESPRESSAS COMO IMPLÍCITAS, INCLUÍNDO AS GARANTIAS IMPLÍCITAS DE MERCADO, FEITAS PARA UM PROPÓSITO EM PARTICULAR, OU NÃO INTERFERÊNCIA, EXACTIDÃO DOS DADOS, EXACTIDÃO DO CONTEÚDO INFORMATIVO, INTEGRAÇÃO DE SISTEMAS, NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS AO FILTRAR, DESACTIVAR OU REMOVER O SOFTWARE DE TERCEIROS, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTOS, PUBLICIDADE OU SEMELHANTE, QUER SURJAM POR ESTATUTO, LEI, NO CURSO DE TRANSAÇÕES, POR COSTUME E HÁBITO, OU USO COMERCIAL.

RENÚNCIA DE DANOS. Qualquer pessoa que use, teste, ou avalie o BitDefender suporta todo o risco pela qualidade e desempenho do BitDefender. A BITDEFENDER não será responsável, em nenhuma circunstância, de qualquer dano de qualquer tipo, incluindo, sem limitação, danos directos ou indirectos provenientes do uso, desempenho, ou entrega do BitDefender, mesmo que a BITDEFENDER tenha sido avisada da existência ou possibilidade de tais danos. ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE DE INCIDENTES OU DANOS CONSEQUENTES, POR ISSO A LIMITAÇÃO ACIMA INDICADA PODERÁ NÃO SE APLICAR A SI. EM NENHUM CASO O RISCO DA BITDEFENDER PODERÁ EXCEDER O PREÇO QUE PAGOU PELO BITDEFENDER. As renúncias e limitações, estabelecidas acima, aplicar-se-ão independentemente se aceita usar, avaliar ou testar o BitDefender.

AVISO IMPORTANTE AOS UTILIZADORES. ESTE SOFTWARE NÃO É À PROVA DE FALHAS E NÃO ESTÁ DESENHADO PARA USO INTENCIONAL EM AMBIENTES DE RISCO QUE REQUEREM UMA PERFORMANCE À PROVA DE FALHAS. ESTE SOFTWARE NÃO ESTÁ INDICADO PARA SER USADO EM OPERAÇÕES DE NAVEGAÇÃO AÉREA, EM INSTALAÇÕES NUCLEARES, OU SISTEMAS DE COMUNICAÇÕES, SISTEMAS DE ARMAMENTO, DIRECTA OU INDIRECTAMENTE EM SISTEMAS DE APOIO À VIDA, CONTROLO DE TRÁFEGO AÉREO, OU QUALQUER APLICAÇÃO OU INSTALAÇÃO, ONDE A FALHA PODE RESULTAR EM MORTE, DANOS FISÍCOS GRAVES OU DANOS DE PROPRIEDADE.

GERAL. Este acordo será regido pelas leis da Roménia e pela regulamentação e tratados internacionais de direitos de autor. A jurisdição e foro exclusivo em caso de

qualquer disputa que surja devido aos Termos desta Licença serão os tribunais da Roménia.

Preços, custos e taxas de uso do BitDefender estão sujeitas a alteração sem qualquer aviso prévio.

Em caso de não-validade de qualquer parte deste Acordo, a não-validade não afecta a validade das restantes partes deste Acordo.

BitDefender e o Logótipo BitDefender são marcas registadas de BITDEFENDER. Todas as outras marcas registadas usadas no produto ou nos materiais associados ao mesmo são propriedade dos respectivos proprietários.

A licença cessará imediatamente e sem aviso se se encontrar a violar qualquer um dos pontos destes termos e condições. Não terá direito a um reembolso por parte de BITDEFENDER ou qualquer um dos revendedores de BitDefender como resultado da cessação da licença. Os termos e condições respeitantes à confidencialidade e restrições em uso manter-se-ão em vigor mesmo após a cessação da licença.

A BITDEFENDER poderá rever estes Termos a qualquer altura e os termos revistos serão automaticamente aplicáveis às versões correspondentes do Software distribuído com os termos revistos. Se qualquer parte destes Termos for encontrada como sendo desnecessária ou inaplicável, essa parte não afectará a validade dos restantes Termos, que permanecerão válidos e aplicáveis.

Em caso de controvérsia ou inconsistência entre as traduções destes Termos e outras línguas, a versão em Inglês emitida pela BITDEFENDER prevalecerá sobre todas as outras.

Contacte BITDEFENDER, em 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, ou pelo Tel No: 0040-21-2330780 ou Fax:0040-21-2330763, e-mail address: office@bitdefender.com.

Prefácio

Este manual é dirigido a todos os utilizadores que escolheram **BitDefender Total Security 2008** como a solução de segurança para o seu computador pessoal. A informação apresentada neste manual é útil e acessível para todas as pessoas que trabalham com o sistema operativo Windows, independentemente do seu nível de conhecimento de informática.

Este manual dá-lhe uma descrição completa do **BitDefender Total Security 2008**, da Empresa e da equipa que o desenvolveu, também irá guiá-lo através do processo de instalação, e explicar-lhe como o pode configurar. Irá ficar a saber como usar o **BitDefender Total Security 2008**, como o actualizar, testar e personalizar. Em resumo, irá ficar a saber como tirar partido do melhor que o BitDefender tem para lhe oferecer.

Desejamos-lhe uma leitura proveitosa e agradável.

1. Convenções Usadas neste Manual

1.1. Convenções Tipográficas

Diversos estilos de texto são usados neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.

Aparência	Descrição
`sample syntax`	Exemplos de sintaxe são impressos em caracteres `monospace`.
http://www.bitdefender.com	O link URL está a apontar para algum local externo, num servidor http ou ftp.
support@bitdefender.com	Endereços de e-mail são inseridos no texto para contactar a solicitar mais informação.
“Prefácio” (p. xiii)	Este é um link interno, que aponta para uma área dentro do documento.
`filename`	Os ficheiros e as directorias são impressos usando a fonte `monospace`.

Aparência	Descrição
option	Todas as opções de produto são impressas usando caracteres a**cheio**.
`sample code listing`	A listagem de código é impressa com caracteres `monospace`.

1.2. Avisos

Os avisos encontram-se em notas de texto, marcadas graficamente, que lhe dão informação adicional respeitante ao parágrafo em questão.

Nota
A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

Importante
Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, dá-lhe informação bastante importante.

Atenção
Trata-se de informação crítica que deve de tratar com cuidados redobrados. Nada de mal acontecerá se seguir as indicações. Deve lê-la e compreendê-la, porque descreve algo extremamente arriscado.

2. A estrutura do Manual

O manual é composto da várias partes contendo os tópicos principais. Mais ainda, um glossário é fornecido para ajudar a clarificar alguns termos técnicos.

Instalação. Instruções passo a passo para a instalação do BitDefender numa estação de trabalho. Este é um manual bastante completo de instruções sobre como instalar e usar **BitDefender Total Security 2008**. Começando pelos requisitos necessários para uma instalação bem-sucedida, é guiado de seguida através de todo o processo de instalação. No final, é-lhe apresentado o procedimento de remoção para o caso de necessitar desinstalar o BitDefender.

Administração Básica. Descripção de administração básica e manutenção do BitDefender.

Administração de Segurança Avançada. Uma apresentação detalhada das capacidades de segurança fornecida pela BitDefender. Os capítulos explicam em detalhe todas as opções da consola de definições avançadas. É ensinado sobre como configurar e usar todos os módulos BitDefender de forma a proteger efectivamente o seu computador contra todo o tipo de ameaças (malware, spam, hackers, conteúdo inapropriado e por aí fora).

Administração de Backup Avançada. Descripção das definições avançadas de backup. É aqui onde irá aprender como estabelecer e executar as operações de backup, restaurar e gravar.

CD de Emergência BitDefender. Descrição do CD de Emergência BitDefender. Ajuda-o a compreender e a usar as características existentes neste CD de arranque.

Obter Ajuda. Onde procurar e onde pedir ajuda se algo inesperado acontecer.

Glossário. O Glossário tenta explicar alguns termos técnicos ou pouco comuns que irá encontrar nas páginas deste documento.

3. Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificámos e testámos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a melhor documentação possível.

Faça-nos saber enviando um e-mail para documentation@bitdefender.com.

Importante

Por favor escreva toda a sua documentação e e-mails em inglês de forma a que possamos dar-lhes seguimento de forma eficiente.

Instalação

1. Instalação do BitDefender Total Security 2008

A secção de **Instalação do BitDefender Total Security 2008** deste guia do utilizador contém os seguintes tópicos:

- Requisitos do Sistema
- Passos da instalação
- Assistente Inicial de Instalação
- Actualização
- Reparar ou Remover o BitDefender

1.1. Requisitos do Sistema

Para um funcionamento correcto do produto, antes de instalar verifique que um dos seguintes sistemas operativos estão a ser executados no seu computador e que os correspondentes requisitos do sistema estão presentes:

- Sistema Operativo: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (ou superior)
- Cliente de e-mail suportados: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 and 2.0

Windows 2000

- Processador 800 MHz ou superior
- Mínimo 256 MB de Memória RAM (512 MB recomendado)
- Mínimo 60 MB de espaço disponível em disco

Windows XP

- Processador 800 MHz ou superior
- Mínimo 512 MB de Memória RAM (1 GB recomendado)
- Mínimo 60 MB de espaço disponível em disco

Windows Vista

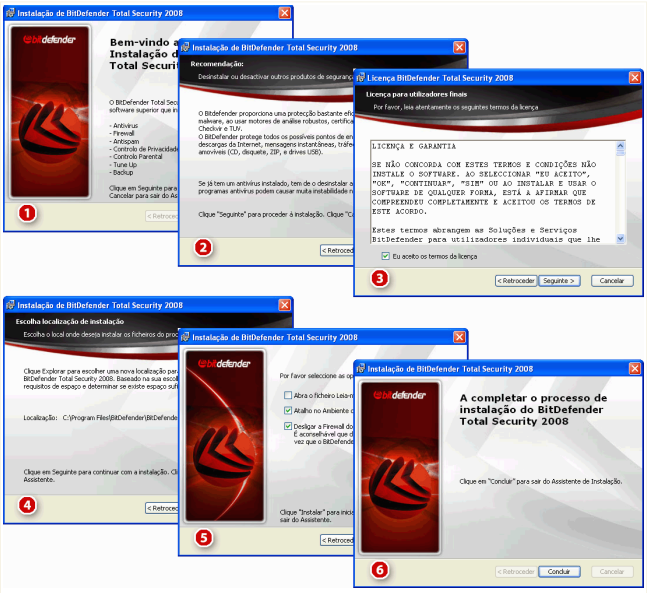
- Processador 800 MHz ou superior
- Mínimo 512 MB de Memória RAM (1 GB recomendado)
- Mínimo 60 MB de espaço disponível em disco

BitDefender Total Security 2008 pode ser descarregado para avaliação a partir do website do BitDefender: http://www.bitdefender.com .

1.2. Passos da Instalação

Localize o ficheiro de instalação (setup) e clique nele duas vezes com o rato. Isto lançará o assistente que o irá guiar através do processo de instalação:

Antes de executar o assistente de instalação, o BitDefender irá verificar se existem novas versões do pacote de instalação. Se uma nova versão estiver disponível, será avisado para o descarregar. Clique **Sim** para descarregar a nova versão ou **Não** para continuar a instalar a versão do ficheiro de instalação.


Instalação de BitDefender Total Security 2008
Licença BitDefender Total Security 2008
Licença para utilizadores finais
Escolha localização de instalação
A completar o processo de instalação do BitDefender Total Security 2008

Passos da Instalação

Siga estes passos para instalar o BitDefender Total Security 2008:

1. Clique em **Seguinte** para continuar ou clique em **Cancelar** se pretende desistir da instalação.
2. Clique em **Seguinte**.

BitDefender Total Security 2008 avisa-o em caso de ter outro produto antivírus instalado no seu computador. Clique em **Remover** para desinstalar o respectivo produto. Se deseja continuar sem remover os produtos detectados, clique em **Seguinte**.

Atenção
É altamente recomendável que desinstale qualquer outro antivírus detectado antes de instalar BitDefender. Usar dois ou mais produtos antivírus ao mesmo tempo num computador pode bloquear totalmente o seu sistema.

3. Por favor leia o Acordo de Licença, seleccione **Eu aceito os termos do Acordo de Licença** e clique em **Seguinte**. Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.
4. Por defeito, o BitDefender Total Security 2008 será instalado em `C:\Programas\BitDefender\BitDefender 2008`. Se deseja seleccionar outra pasta, clique em **Explorar** e seleccionar a pasta onde pretende que o BitDefender Total Security 2008 seja instalado.

   Clique em **Seguinte**.
5. Seleccione as opções que tem a ver com o processo de instalação. Algumas delas serão seleccionadas por defeito:
   - **Abrir o ficheiro Leia-me** - para abrir o ficheiro Leia-me no final da instalação.
   - **Colocar um atalho no ambiente de trabalho** - para colocar um atalho do BitDefender Total Security 2008, no seu ambiente de trabalho, no final da instalação.
   - **Ejectar o CD quando a instalação terminar** - para obter que o CD seja ejectado no final da instalação esta opção aparece quando instala o produto a partir do CD.
   - **Desligar a Firewall do Windows** - para desligar a Firewall do Windows.

     Importante
     Recomendamos que desligue a Firewall do Windows uma vez que BitDefender Total Security 2008 já inclui uma firewall avançada. Executar 2 firewalls no mesmo computador poderá causar problemas.

   - **Desligar o Windows Defender** - para desligar o Windows Defender; esta opção apenas surge no Windows Vista.

   Clique em **Instalar** de forma a iniciar a instalação do produto.

Importante

Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu**BitDefender Total Security 2008**, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.
Complete o processo guiado pelo assistente de forma a seguir para o próximo passo.

6. Clique em **Terminar**. Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação. Recomendamos que o faça assim que seja possível.

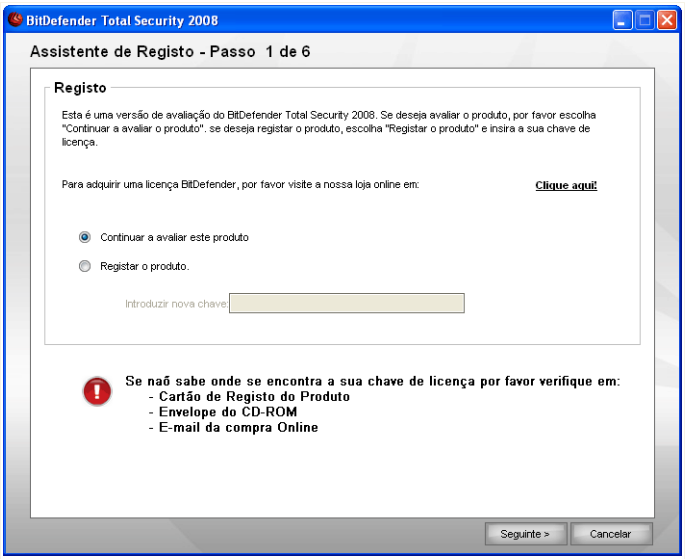
   Se aceitou as definições por defeito do caminho da instalação, poderá ver uma pasta com o nome `BitDefender` nos `Programas` que contém a subpasta `BitDefender 2008`.

1.3. Assistente Inicial de Instalação

Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu**BitDefender Total Security 2008**, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.

Completar a acção do assistente não é obrigatória; no entanto, recomendamos que a termine de forma a poupar tempo e a assegurar que o seu sistema fica seguro ainda antes do BitDefender Total Security 2008 estar instalado.

1.3.1. Passo 1/6 - Registar o BitDefender Total Security 2008


BitDefender Total Security 2008
Assistente de Registo - Passo 1 de 6
Registo
Esta é uma versão de avaliação do BitDefender Total Security 2008. Se deseja avaliar o produto, por favor escolha "Continuar a avaliar o produto". se deseja registar o produto, escolha "Registar o produto" e insira a sua chave de licença.
Para adquirir uma licença BitDefender, por favor visite a nossa loja online em:
Clique aqui!
Continuar a avaliar este produto
Registar o produto.
Introduzir nova chave:
Se naõ sabe onde se encontra a sua chave de licença por favor verifique em:
- Cartão de Registo do Produto
- Envelope do CD-ROM
- E-mail da compra Online
Seguinte >
Cancelar

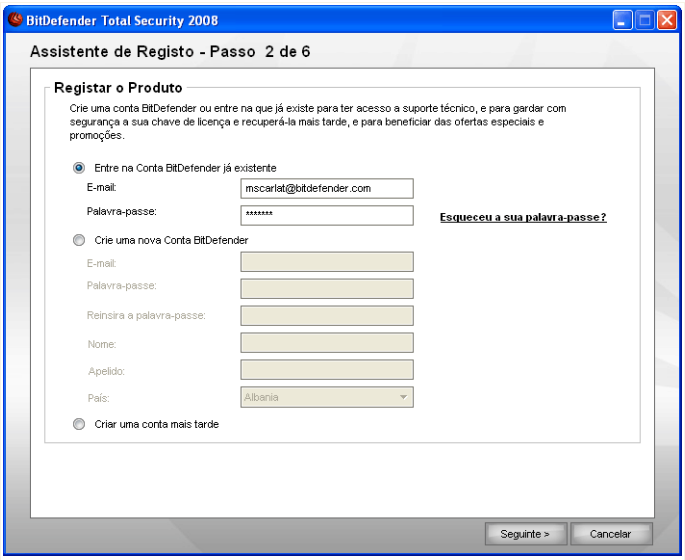
Registo

Escolha **Registar o produto** para registar o**BitDefender Total Security 2008**. Insira a chave de licença no campo **Introduzir nova chave**.

Para continuar a avaliar o produto, seleccione **Continuar a avaliar o produto**.

Clique em **Seguinte**.

1.3.2. Passo 2/6 - Criar uma conta BitDefender


BitDefender Total Security 2008
Assistente de Registo - Passo 2 de 6
Registar o Produto
Crie uma conta BitDefender ou entre na que já existe para ter acesso a suporte técnico, e para gardar com segurança a sua chave de licença e recuperá-la mais tarde, e para beneficiar das ofertas especiais e promoções.
Entre na Conta BitDefender já existente
E-mail:
mscarlat@bitdefender.com
Palavra-passe:
****
Esqueceu a sua palavra-passe?
Crie uma nova Conta BitDefender
E-mail:
Palavra-passe:
Reinsira a palavra-passe:
Nome:
Apelido:
País:
Albania
Criar uma conta mais tarde
Seguinte >
Cancelar

Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Nota
Se deseja criar uma conta mais tarde, selecciona a devida opção.

Para criar uma conta BitDefender seleccione**Criar uma nova conta BitDefender** e forneça a devida informação. Os dados que nos fornecer serão mantidos confidenciais.

- **E-mail** - insira o seu endereço de e-mail.
- **Palavra-passe** - introduza uma palavra-passe para a sua conta BitDefender.

Nota
A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

- **Reinsira a palavra-passe** - introduza novamente a palavra-passe que previamente definiu.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - seleccione o país em que reside.

Nota
Use o endereço de e-mail e a palavra-passe que forneceu para fazer log à sua conta em http://myaccount.bitdefender.com.

Para criar com sucesso uma conta deverá em primeiro lugar activar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para si pelo serviço de registo da BitDefender.

Clique em **Seguinte** para continuar.

Já tenho uma conta BitDefender

BitDefender detectará automaticamente se já possui uma conta BitDefender previamente registada no seu computador. Nesse caso, tudo o que tem de fazer é clicar em **Seguinte**.

Se já possui uma conta activa, mas o BitDefender não a detecta, seleccione**Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a palavra-passe da sua conta.

Nota
Se forneceu a palavra-passe incorrecta, será notificado para a re-inserir quando clicar em **Seguinte**. Clique em **OK** para inserir a apalavra-passe novamente ou **Cancelar** para sair do assistente.

Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

Clique em **Seguinte** para continuar.

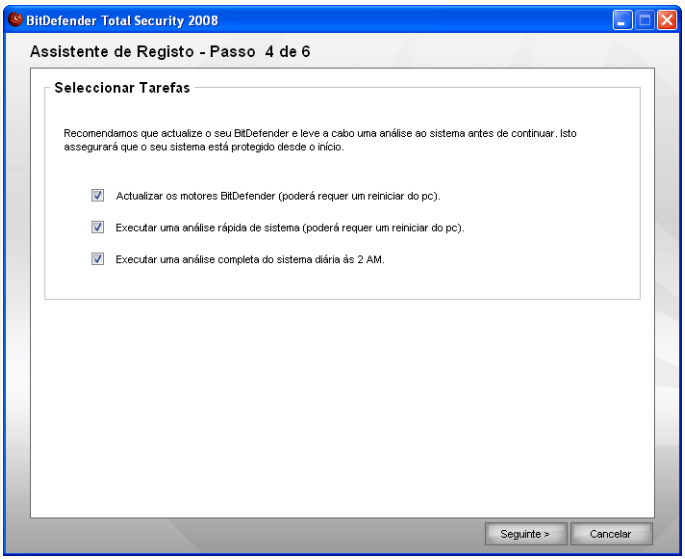
1.3.3. Passo 3/6 - Saber mais acerca de RVTR (Relatório de Vírus em Tempo Real)

BitDefender Total Security 2008
Assistente de Registo - Passo 3 de 6
Configuração
O Real Time Virus Reporting (Relatório de Vírus em Tempo-Real) e os módulos Outbreak Detection (Detecção de Epidemias) reportam o nome do seu país, os nomes dos vírus, o número de vírus encontrados e os ficheiros analisados e a informação acerca de processos executados para o Laboratório BitDefender. Este relatório não contém qualquer informação pessoal. O worldwide Virus Map (Mapa de Vírus mundial) que pode ser consultado em http://www.bitdefender.com é compilado usando essa informação.
Se desejar desactivar estes módulos, pode fazê-lo, após instalar e desmarcar as opções "Enviar relatórios de vírus" e "Activar BitDefender Detecção de Epidemias" a partir da secção Configuração > Avançada.
Seguinte >
Cancelar

Informação de RVTR

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.4. Passo 4/6 - Seleccionar as Tarefas a Serem Executadas


BitDefender Total Security 2008
Assistente de Registo - Passo 4 de 6
Seleccionar Tarefas
Recomendamos que actualize o seu BitDefender e leve a cabo uma análise ao sistema antes de continuar. Isto assegurará que o seu sistema está protegido desde o início.
Actualizar os motores BitDefender (poderá requer um reiniciar do pc).
Executar uma análise rápida de sistema (poderá requer um reiniciar do pc).
Executar uma análise completa do sistema diária às 2 AM.
Seguinte >
Cancelar

Selecção das Tarefas

Preparar o BitDefender Total Security 2008 para levar a cabo tarefas importantes para a segurança do seu sistema.

Estão disponíveis as seguintes opções:

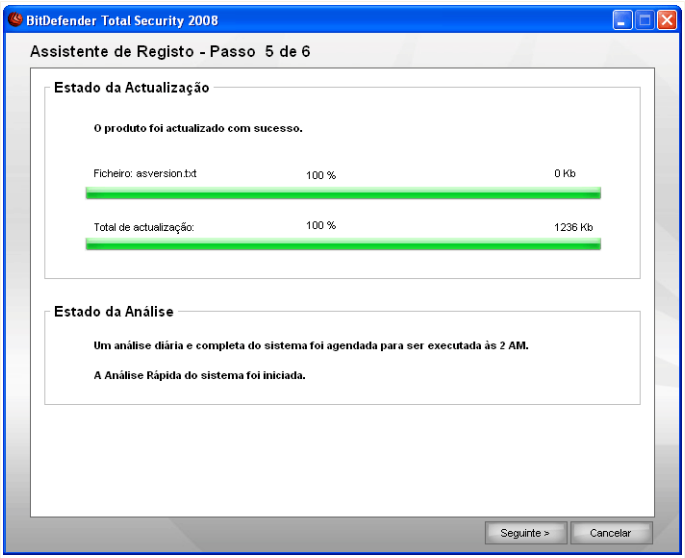
- **Actualizar os motores BitDefender (poderá ser necessário reiniciar)** - durante o próximo passo, será efectuada a actualização dos motores BitDefender de forma a proteger o seu computador contra as ameaças mais recentes.
- **Executar uma análise rápida do sistema (poderá ser necessário reiniciar)** - durante o próximo passo, uma análise rápida do sistema será executada de forma a que o BitDefender se certifique que os seus ficheiros das pastas `Windows` e `Programas` não estão infectados.
- **Executar uma análise completa diária às 2 AM** - Executa uma análise completa diária às 2 AM.

Importante
Recomendamos que tenha estas opções activas antes de avançar para o próximo passo de forma a assegurar a segurança do seu sistema.

Se seleccionar apenas a última opção ou nenhuma opção, irá saltar o próximo passo.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.5. Passo 5/6 - Esperar que as Tarefas Terminem

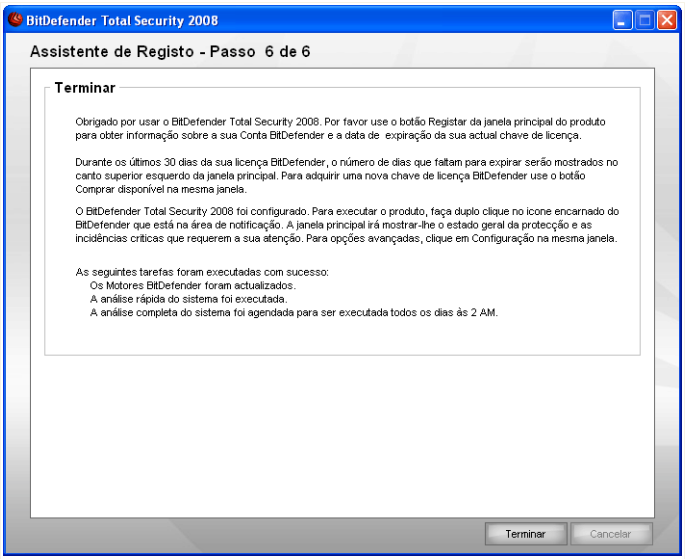

BitDefender Total Security 2008
Assistente de Registo - Passo 5 de 6
Estado da Actualização
O produto foi actualizado com sucesso.
Ficheiro: asversion.txt
100 %
0 Kb
Total de actualização:
100 %
1236 Kb
Estado da Análise
Um análise diária e completa do sistema foi agendada para ser executada às 2 AM.
A Análise Rápida do sistema foi iniciada.
Seguinte >
Cancelar

Estado das Tarefas

Esperar que as tarefas terminem. Pode ver o estado das tarefas seleccionadas no passo anterior.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

1.3.6. Passo 6/6 - Ver Resumo


BitDefender Total Security 2008
Assistente de Registo - Passo 6 de 6
Terminar
Obrigado por usar o BitDefender Total Security 2008. Por favor use o botão Registar da janela principal do produto para obter informação sobre a sua Conta BitDefender e a data de expiração da sua actual chave de licença.
Durante os últimos 30 dias da sua licença BitDefender, o número de dias que faltam para expirar serão mostrados no canto superior esquerdo da janela principal. Para adquirir uma nova chave de licença BitDefender use o botão Comprar disponível na mesma janela.
O BitDefender Total Security 2008 foi configurado. Para executar o produto, faça duplo clique no ícone encarnado do BitDefender que está na área de notificação. A janela principal irá mostrar-lhe o estado geral da protecção e as incidências críticas que requerem a sua atenção. Para opções avançadas, clique em Configuração na mesma janela.
As seguintes tarefas foram executadas com sucesso:
Os Motores BitDefender foram actualizados.
A análise rápida do sistema foi executada.
A análise completa do sistema foi agendada para ser executada todos os dias às 2 AM.
Terminar
Cancelar

Terminar

Este é o passo final do assistente de configuração.

Clique em **Terminar** para completar a acção do assistente e continuar com o processo de instalação.

1.4. Upgrade (Mudança de versão)

O procedimento de upgrade (mudança de versão) pode ser feito de uma das seguintes formas:

- **Instalar sem remover a versão anterior – para a v8 ou superior, excepto o Internet Security**

  Faça duplo-clique no ficheiro de instalação e siga o assistente descrito na secção "*Passos da Instalação*" (p. 3).

Importante
Durante o processo de instalação uma mensagem de erro causada pelo `serviço Filespy`, irá aparecer. Clique em **OK** para continuar com a instalação.

- **Desinstale a sua anterior versão e instale a nova – para todas as versões BitDefender**

  Em primeiro, lugar tem de remover a anterior versão, reiniciar o computador e instalar a nova versão tal como descrito na secção "*Passos da Instalação*" (p. 3).

Importante
Se está a mudar de versão a partir de BitDefender v8 ou superior, recomendamos que guarde a configuração BitDefender, a lista de Amigos e a lista de Spammers. Após o processo de mudança de versão estar concluído, poderá carregá-las.

1.5. Remover ou Reparar o BitDefender

Se pretende reparar ou desinstalar o **BitDefender Total Security 2008**, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2008** → **Reparar ou Desinstalar**.

Irá ser-lhe pedido para confirmar a sua opção ao clicar em **Seguinte**. Irá aparecer uma nova janela, na qual pode seleccionar:

- **Reparar** - para reinstalar todos os componentes já instalados no passo anterior;

Importante
Antes de reparar o produto recomendamos que guarde a lista de Amigos e a lista de Spammers. Pode também guardar a configuração BitDefender e a base de dados Bayesiana. Após terminar o processo de reparação poderá carregá-las novamente.

  Se escolher reparar o BitDefender, surgirá uma nova janela. Clique em **Reparar** para dar início ao processo de reparação.

  Reinicie o computador quando tal lhe for solicitado, e depois, clique em **Instalar** para reinstalar BitDefender Total Security 2008.

  Uma vez terminado o processo de intalação, surgirá uma nova janela. Clique em **Terminar**.
- **Remover** - para remover todos os componentes instalados.

Nota
Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

Se escolher desinstalar BitDefender, surgirá uma nova janela.

Importante

Ao remover o BitDefender, deixará de estar protegido contra os vírus, spyware e os hackers. Se deseja que a Firewall do Windows e o Windows Defender sejam activados após desinstalar o BitDefender, seleccione as correspondentes caixas de selecção durante o próximo passo.

Clique em **Desinstalar** para dar início à desinstalação do BitDefender Total Security 2008 do seu computador.

Durante o processo de desinstalação será solicitado o seu feedback. Por favor clique em **OK** para responder a um inquérito online que consiste apenas de cinco pequenas perguntas. Se não pretender responder ao inquérito clique em **Cancelar**.

Uma vez terminada a desinstalação, surgirá uma nova janela. Clique em **Terminar**.

Nota

Quando o processo de desinstalação tiver terminado, recomendamos que elimine a pasta `BitDefender` dos `Programas`.

Ocorreu um erro ao desinstalar o BitDefender

Se ocorrer um erro ao desinstalar o BitDefender, o processo de desinstalção será cancelado e surgirá uma nova janela. Clique **Desinstalar** para se certificar que o BitDefender foi removido completamente. A Ferramenta de Desinstalação removerá todos os ficheiros e chaves de registo que não tenham sido removidos durante o processo de desinstalação automática.

Administração Básica

2. Introdução

Uma vez que tenha instalado BitDefender o seu computador fica protegido. Pode abrir o Centro de Segurança BitDefender e verificar o estado de segurança do sistema, tomar medidas preventivas ou configurar o produto na sua totalidade em qualquer altura.

Para aceder ao Centro de Segurança BitDefender, use o menu do Iniciar do Windows, seguindo o caminho **Iniciar → Programas → BitDefender 2008 → BitDefender Total Security 2008**ou mais rapidamente, duplo clique no **ícone BitDefender** que está na área de notificação.

Centro de Segurança BitDefender

O Centro de Segurança BitDefender contém duas áreas:

- O **Estado** da área: contém informaçãoe ajuda-o a reparar as vulnerabilidades de segurança do seu computador. Pode facilmente ver quantas incidências poderão estar a afectar o seu computador. Ao clicar no botão vermelho correspondente a **Reparar Todas Incidências** as vulnerabilidades do seu computador serão resolvidas

na hora ou será orientado no sentido de as resolver facilmente. Ao mesmo tempo, quatro botões de estado correspondentes a quatro categorias de segurança estão disponíveis. Botões de estado verdes indicam que não há risco. Botões amarelos ou vermelhos indicam risco de segurança médios ou elevados. Para os reparar, clique no botão amarelo/vermelho, e depois nos botões **Reparar**, uma a um ou no botão **Reparar tudo agora**. Cinzento indica um componente não configurado.

- A área de **Tarefas Rápidas**: ajuda-o a tomar medidas preventivas essenciais para manter o seu sistema seguro e proteger a sua informação. Consistes de três barras correspondentes a três tipos de acções de segurança. Aqui pode actualizar o seu produto, analisar o seu computador, fazer backup ou restaurar os seus dados, defragmentar o seu disco, limpar ficheiros temporários da internet e cookies, limpar e recuperar o registo, encontrar ficheiros duplicados como também apagar ficheiros em segurança.

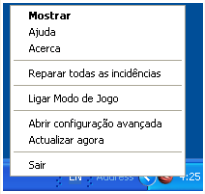
E mais ainda, o Centro de Segurança BitDefender contém diversos atalhos úteis.

Link	*Descrição*
Comprar	Abre uma página web de onde pode comprar o produto.
Minha Conta	Abrir a página da sua conta BitDefender.
Registar	Abrir o assistente de registo.
Ajuda	Abre o ficheiro de ajuda.
Suporte	Abre a página web do suporte BitDefender.
Configuração	Abre a consola de configuração avançada.
Histórico	Abre uma janela com o histórico BitDefender & eventos.

2.1. Ícone BitDefender na Área de Notificação

Para gerir todo o produto mais rapidamente, pode também usar o icone BitDefender na Área de Notificação.

Se fizer duplo-clique neste ícone, o Centro de Segurança BitDefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender:



Icone BitDefender

- **Mostrar** - abre o o Centro de Segurança BitDefender.
- **Ajuda**- abre o ficheiro de ajuda.
- **Acerca** - abre a página web do BitDefender.
- **Reparar todos incidências** - ajuda-o a removeras vulnerabilidades de segurança.
- **Ligar / desligar Modo de Jogo** - Liga/desliga Modo de Jogo .
- **Abrir Configuração Avançada** dá-lhe acesso à consola de configuração avançada.
- **Actualizar agora** - executa uma actualização imediata. Surge uma nova janela, onde pode ver o estado da actualização.
- **Sair** - desliga a aplicação.

Sempre que o Modo de Jogo está ligado, pode ver a letra G sobre o ícone BitDefender.

Se existem incidências criticas que afectam a segurança do seu sistema, um ponto de exclamação é mostrado por cima do ícone do BitDefender. Pode passar com o rato por cima do icone para ver o número de incidências que estão a afectar a segurança do seu sistema.

2.2. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade da análise no seu sistema.

As barras verdes (a **zona PC**) mostram o número de ficheiros analisados por segundo, numa escala de 0 a 50.

As barras vermelhas apresentadas na **zona Net** mostram o número de Kbytes transferidos (enviados e recebidos da Internet) a cada segundo, numa escala de 0 a 100.

Barra de Actividade

Nota

A barra de actividade da Análise avisa-o quando a protecção em Tempo-real ou a Firewall está desactivada ao mostrar uma cruz vermelha sobre a área correspondente (**zona PC** ou **zona Net**).

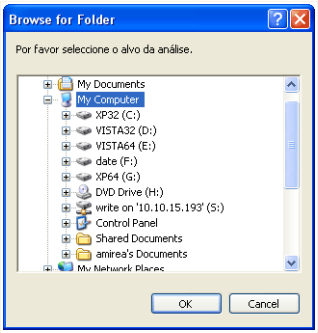
Pode usar a **Barra de Actividade da Análise** para analisar objectos. Apenas arraste os objectos que deseja analisar para cima dela. Para mais informação, por favor consulte o "*Análise por Drag&Drop*" (p. 100).

Quando quiser deixar de ver o gráfico de visualização, faça clique com o botão direito do rato sobre ele e seleccione **Esconder**. Para esconder completamente esta janela, clique **Avançada** na consola de configuração e limpe a caixa de selecção correspondente a **Activar a Barra de Actividade da Análise (gráfico no ecrãn)**.

2.3. Análise Manual BitDefender

Se deseja analisar rapidamente uma determinada pasta, pode usar a Análise Manual BitDefender.

Para aceder à Análise Manual BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2008** → **Análise Manual BitDefender**. A seguinte análise irá aparecer:



Análise Manual BitDefender

Tudo o que tem de fazer é explorar as pastas, seleccionar a que deseja analisar e clicar **OK**. O Analisador BitDefender irá surgir e guiá-lo através do processo de análise.

2.4. Modo de Jogo

O novo Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema. Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.

- A Firewall BitDefender está definida em **Modo de Jogo**.

Sempre que o Modo de Jogo está ligado, pode ver a letra `G` sobre o ícone BitDefender.

2.4.1. Usar o Modo de Jogo

Se deseja ligar o Modo de Jogo, pode usar um dos seguintes métodos:

- Clique com o botão-direito do rato no ícone do BitDefender que está na área de notificação e seleccione **Ligar Modo de Jogo**.
- Prima `Alt+G` (A hotkey por defeito).

Importante
Não se esqueça de desligar o Modo de Jogo quando terminar. Para fazer isto, use os mesmos processos que usou para o ligar.

2.4.2. Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

1. Clique em **Configuração** - no Centro de Segurança BitDefender para abrir a consola de configuração.

   Nota
   Pode clicar com o botão direito do rato no ícone do BitDefender que está na área de notificação e seleccione **Configuração Avançadas**.

2. Clique em **Avançada**.
3. Por baixo da opção **Activar HotKey do Modo de Jogo** , defina a hotkey desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar a hotkey `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.

   Nota
   Remover a selecção ao pé de **Activar HotKey para o Modo de Jogo** irá desactivar a hotkey.

3. Estado de Segurança

O estado de segurança mostra uma lista de segurança sistematicamente organizada e de fácil gestão do seu computador. O BitDefender Total Security 2008 irá informá-lo sempre que exista um problema que possa afectar a segurança do seu computador.

Existem quatro botões de estados de segurança:

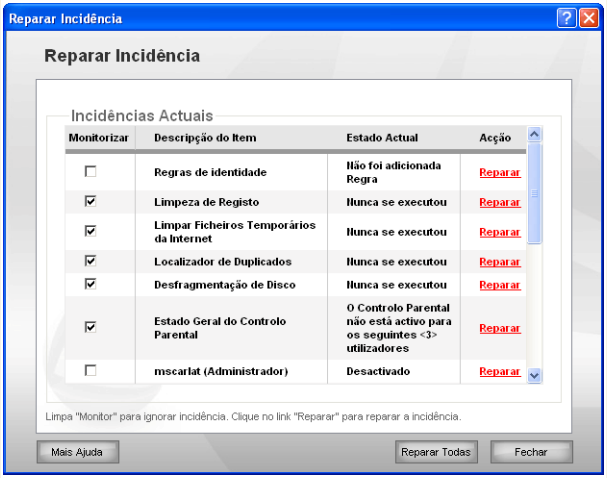
- **SEGURANÇA**
- **CONTROLO PARENTAL**
- **TUNEUP**
- **BACKUP**

Ao mesmo tempo, à esquerda pode ver o número de incidências que estão a afectar a segurança do seu sistema e um botão vermelho para**Reparar Todas Incidências**.

Os quatro botões de estado, podem estar a verde, amarelo, vermelho ou cinzento, dependendo do actual nível de protecção.

- **Verde** indica um baixo risco de segurança para o seu computador.
- **Amarelo** indica um médio risco de segurança para o seu computador.
- **Vermelho** indica um elevado risco de segurança para o seu computador.
- **Cinzento** indica um componente não-configurado.

Reparar os problemas de segurança não requer qualquer esforço e pode ser feito com um simples click em **Reparar Todas Incidências**. Uma nova janela irá aparecer.



Incidências de Segurança

Verá uma lista das incidências de segurança e uma pequena descripção do seu estado.

Para reparar apena uma incidência em particular clique no botão correspondente **Reparar**. Será resolvida logo aí ou seguindo os passos de um assistente. Se decidir repará-los a todos, clique no botão **Reparar Todas Agora** e siga o assistente correspondente.

Se necessita de ajuda adicional, clique no botão **Mais Ajuda**, localizado no fundo da janela. Uma página de ajuda contextual é mostrada dando-lhe mais informação detalhada sobre as incidências e a forma de as reparar.

Importante

Para cada incidência, existe uma caixa de selecção, activada por defeito. Se não deseja que uma determinada incidência seja tomada em consideração quando é calculado o risco de segurança, limpe a correspondente caixa de selecção. Por favor use esta opção com cuidado, porque é muito fácil aumentar o risco de segurança a que o seu computador está exposto.

Para reparar as incidências mais tarde, clique **Fechar**.

3.1. Botão De Estado De Segurança

Se o botão de estado de segurança estiver verde, não há nada com que se preocupar. Por outro lado se o botão estiver amarelo, vermelho ou cinzento, existe um risco de segurança médio ou elevado a que o seu computador está exposto.

A cor dos botões de estado podem mudar não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes. Por exemplo, se a última análise ao sistema for antiga, o botão de estado de segurança ficará amarelo. Se for muita antiga, ficará vermelho.

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	*Cor*
A última análise ao sistema é antiga	Amarelo
A última análise ao sistema é muito antiga	Vermelho
A protecção em tempo-real está desactivada	Vermelho
O nível da protecção antivírus foi definido como permissivo	Amarelo
A protecção de privacidade está desactivada	Vermelho
A firewall está desactivada	Vermelho
O modo stealth está desactivado	Vermelho
A ligação wireless não é segura	Vermelho
A actualização automática está desactivada	Vermelho
A última actualização tem um dia	Vermelho
O antispam está desactivado	Cinzento

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado de segurança.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

3.2. Botão de Estado do Controlo Parental

Se o botão de estado do Controlo Parental estiver verde, o mesmo está activado. Se estiver cinzento, está desactivado.

Para activar o Controlo Parental, siga estes passos:

1. Clique no botão de estado do Controlo Parental.
2. Faça o seguinte:
   - Para activar o Controlo Parental para todos os utilizadores, clique em **Reparar Todas**.
   - Para activar o Controlo Parental apenas para um utilizador específico clique no botão **Reparar** correspondente a esse utilizador.

3.3. Botão de Estado TuneUp

Se o botão de estado do tuneup estiver verde, não há nada com que se preocupar. Por outro lado, se o botão estiver amarelo ou vermelho, existe um risco médio ou elevado de segurança ao qual o seu computador está exposto.

A cor dos botões de estado podem mudar não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes.

Por exemplo, se a última desfragmentação do seu computador for muito antiga, o botão de estado de segurança ficará vermelho.

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	*Cor*
A última limpeza de ficheiros internet e cookies é antiga	Amarelo
A última limpeza de ficheiros internet e cookies é muito antiga	Vermelho
A última limpeza do registo é antiga	Amarelo
A última limpeza do registo é muito antiga	Vermelho
A última limpeza de ficheiros duplicados é antiga	Amarelo
A última desfragmentação é antiga	Amarelo
A última desfragmentação é muito antiga	Vermelho

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado do tuneup.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Nota
Para mais informação acerca destes assistentes, consulte a secção "*TuneUp*" (p. 43) .

3.4. Botão de Estado do Backup

Se o botão do estado do backup está verde, não há nada com que se preocupar. Por outro lado, se o botão estiver amarelo ou vermelho, existe um risco médio ou elevado de segurança ao qual o seu computador está exposto.

A cor dos botões de estado podem mudar não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes.

Por exemplo, se o último backup que fez do seu computador for muito antigo o estado de segurança ficará vermelho.

A tabela abaixo dar-lhe-á informação acerca de quais os elementos a serem tomados em conta no cálculo do risco de segurança.

Incidência	*Cor*
O último backup dos dados é antigo	Amarelo
O último backup dos dados é muito antigo	Vermelho

Para reparar as incidências, siga os seguintes passos:

1. Clique no botão de estado do backup.
2. Clique nos botões **Reparar** para reparar as incidências uma a uma ou no botão **Reparar Todos Agora** para as reparar todas de uma só vez.
3. Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Nota
Para mais informação sobre estes assistentes, consulte a secção "*Backup*" (p. 34) .

4. Tarefas Rápidas

Existem três barras debaixo dos quatro botões de estado que correspondem a três tipos de tarefas de segurança:

- **Segurança**
- **Backup**
- **TuneUp**

4.1. Segurança

BitDefender traz consigo um módulo de Segurança que ajuda-o a manter o seu BitDefender actualizado e o seu computador livre de vírus.

Para entrar no módulo de Segurança, clique na barra **Segurança**.

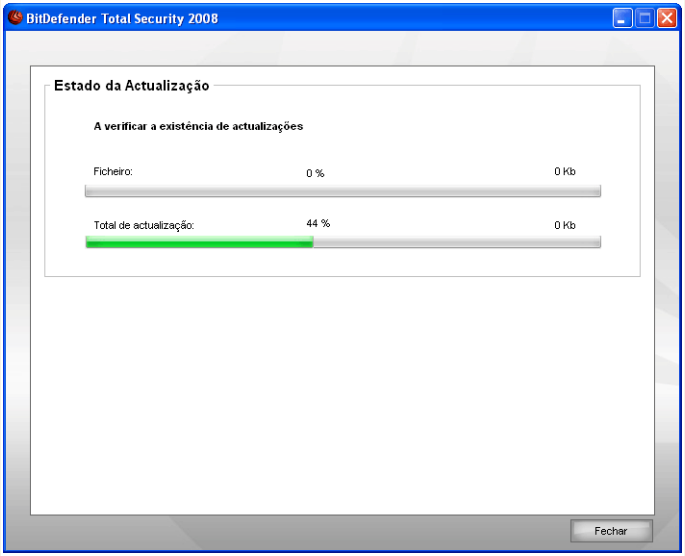
Estão disponíveis os seguintes botões:

- **Actualizar agora** - executa uma actualização imediata.
- **Analisar os Meus Documentos** - inicia uma análise rápida à sua pasta Documents and Settings.
- **Análise Minuciosa do Sistema** - inicia uma análise minuciosa ao seu computador.
- **Análise Completa do Sistema** - inicia uma análise completa ao seu computador.

4.1.1. Actualizar o BitDefender

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware.

Por defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . No entanto, se deseja actualizar o BitDefender, clique em **Actualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Actualizar o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Se deseja fechar esta janela, clique em **Fechar**. No entanto, isso não irá parar o processo de actualização.

Nota
Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

Reinicie o computador se requerido. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador: Se não deseja ser mais notificado novamente quando uma actualização necessitar de reiniciar o seu pc, seleccione **Esperar pelo reiniciar, em vez de me avisarem**. Desta forma, da próxima vez que uma actualização necessitar de reiniciar o pc, o produto continuará a funcionar com os ficheiros antigos até que reinicie o seu sistema.

Clique em **Reiniciar** para reiniciar o seu sistema imediatamente.

Se deseja reiniciar o seu sistema mais tarde, clique apenas em **OK**. Recomendamos que reinicie o seu sistema o mais rápido possível.

4.1.2. A analisar com BitDefender

Para analisar o seu computador em busca de malware, execute uma tarefa de análise em particular, clicando no respectivo botão. A seguinte tabela aprsenta todas as tarefas disponíveis, com uma descrição de cada uma delas:

Tarefa	*Descrição*
Analisar Os Meus Documentos	Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto assegurará a segurança dos seus documentos, um espaço de trabalho seguro e aplicações limpas que se executam durante o iniciar do windows.
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Nota

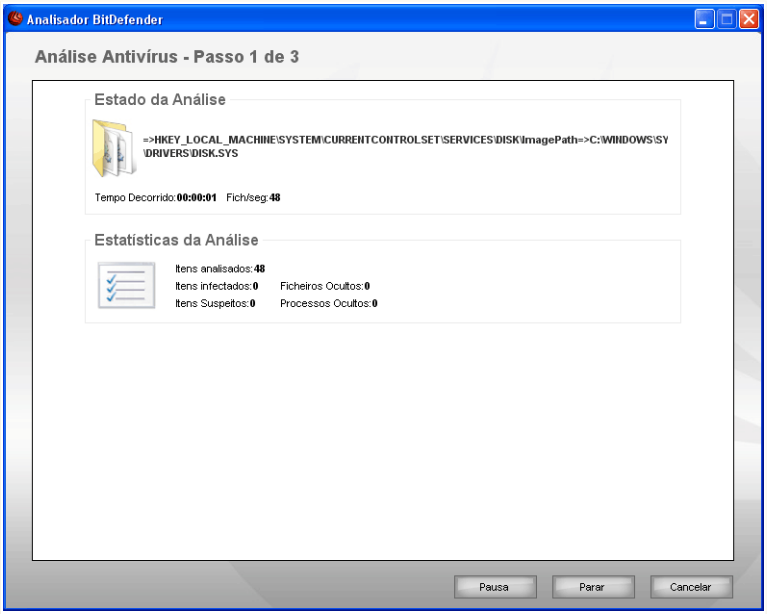
Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

Quando dá início a um processo de análise a-pedido, quer seja uma análise rápida ou completa, o Analisador BitDefender surgirá.

Siga o processo guiado de três passos para completar o processo de análise.

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

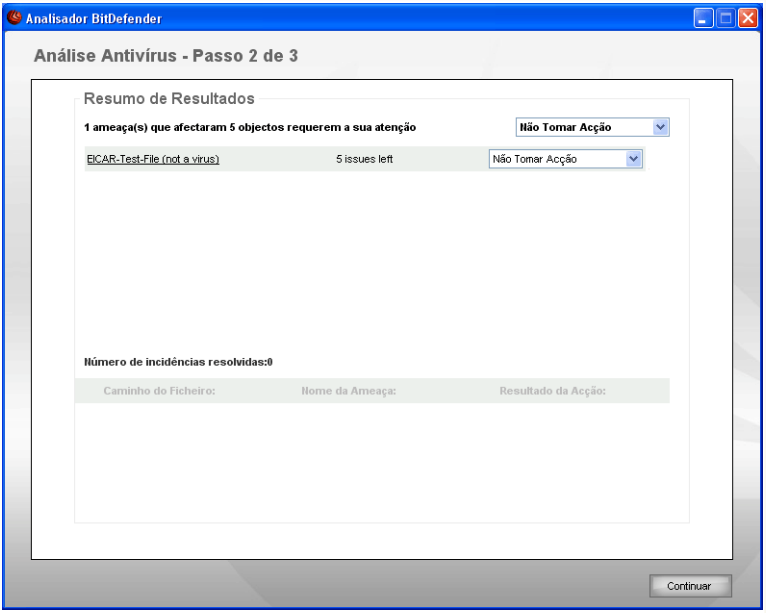
Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá directamente para o último passo do assistente.

Espere que o BitDefender termine a análise.

Passo 2/3 - Seleccionar as acções

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.



Acções

Pode ver o número de incidências que afectam o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Pode escolher uma acção geral a ser tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

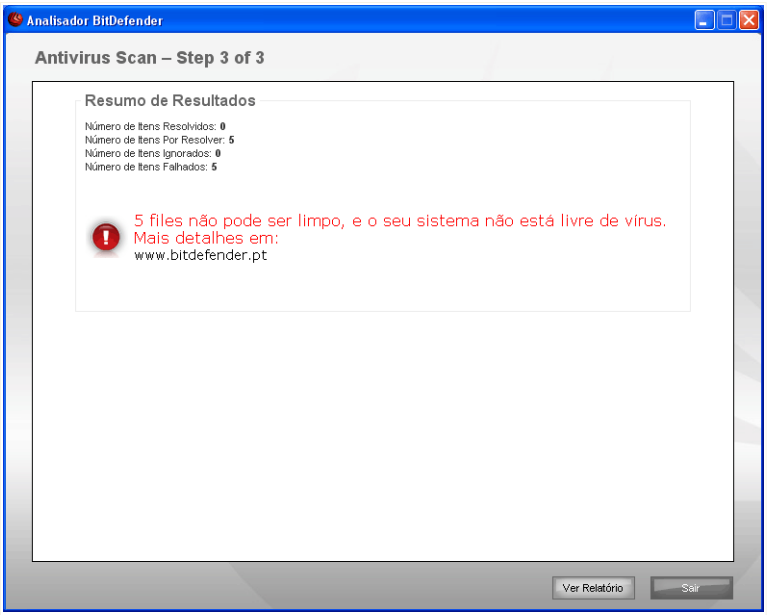
As seguintes opções podem aparecer no menu:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados.
Desinfectar	Desinfecta os ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Desocultar	Torna visíveis objectos ocultos.

Clique em **Continuar** para aplicar as acções especificadas.

Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.


Analisador BitDefender
Antivirus Scan – Step 3 of 3
Resumo de Resultados
Número de Itens Resolvidos: 0
Número de Itens Por Resolver: 5
Número de Itens Ignorados: 0
Número de Itens Falhados: 5
5 files não pode ser limpo, e o seu sistema não está livre de vírus.
Mais detalhes em:
www.bitdefender.pt
Ver Relatório
Sair

Resumo

Pode ver o resumo dos resultados. O ficheiro do relatório é guardado automaticamente na secção de Logs a partir da janela **Propriedades** da respectiva tarefa.

Importante
Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação.

Clique em **Sair** para fechar a janela.

BitDefender Não pode Resolver Algumas Incidências

Na maioria dos casos BitDefender desinfecta com sucesso os ficheiros infectados ou isola a infecção. No entanto, há incidências que não podem ser resolvidas.

Se existirem incidências não resolvidas, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.pt. O nosso suporte técnico ajuda-lo-á a resover as incidências que está a experimentar.

BitDefender Detectou Itens protegidos por Palavra-passe

A categoria de protegidos por palavra-passe inclui dois tipos de itens: arquivos e instaladores. Eles não representam uma verdadeira ameça à segurança do sistema a não ser que contenham ficheiros infectados e apenas quando são executados.

Para ter a certeza de que estes itens estão limpos:

- Se o item protegido por palavra-passe for um arquivo que protegeu com uma palavra-passe, extraia os ficheiros do mesmo e analise-os separadamente. A forma mais fácil de os analisar é clique botão-direito do rato sobre eles e seleccionar **BitDefender Antivirus 2008** a partir do menu.
- Se o item protegido por palavra-passe for um instalador, certifique-se que a protecção em tempo-real está activa antes de executar esse mesmo instalador. Se o instalador estiver infectado, o BitDefender detectará a situação e isolará a infecção.

Se não deseja que estes objectos sejam detectados novamente pelo BitDefender tem de os adiconar como excepções ao processo de análise. Para adicionar excepções à análise, clique em, **Definições** para abrir a consola das configurações e depois vá para **Antivírus > Excepções** . Para mais informação, consulteObjectos Excluídos da Análise

BitDefender Detectou Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

Se foram detectados ficheiros suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender. Clique **OK** para enviar estes ficheiros para uma análise mais avançada no laboratório do BitDefender.

4.2. Backup

BitDefender vem com um módulo de Backup que o ajuda a fazer cópias de reserva de todos os dados valiosos no seu sistema. Pode fazer backup para o seu computador, discos amovíveis ou para uma localização de rede para se certificar que os pode restaurar quando necessário. O restauro dos seus dados é um processo muito fácil.

Para entrar no módulo de Backup clique na barra **Backup** debaixo dos quatro botões de estado.

Estão disponíveis os seguintes botões:

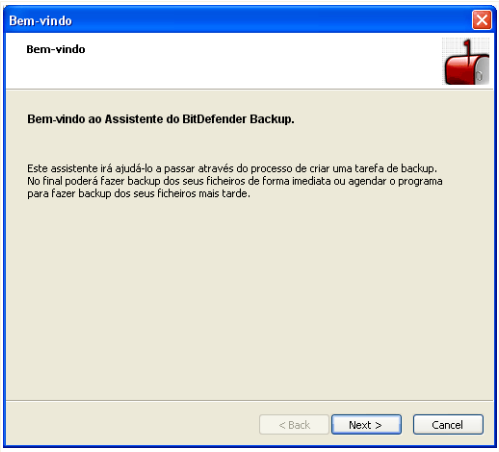
- **Iniciar o Assistente de Backup** - inicia um procedimento de cinco passos para fazer um backup dos seus dados.
- **Configuração Avançada** - aqui é onde pode definir e executar operações de backup em detalhe.
- **Iniciar Assistente de Restauro** - inicia um procedimento de quatro passos para restaurar os seus dados.

4.2.1. Iniciar Assistente de Backup

Ao clicar em **Iniciar Assistente de Backup** irá aparecer-lhe um assistente que o irá levar através de um processo de criação de uma tarefa de backup. No final do processo será capaz de fazer backup dos seus dados na hora ou agendar o produto para o fazer mais tarde.

Passo 1/5 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

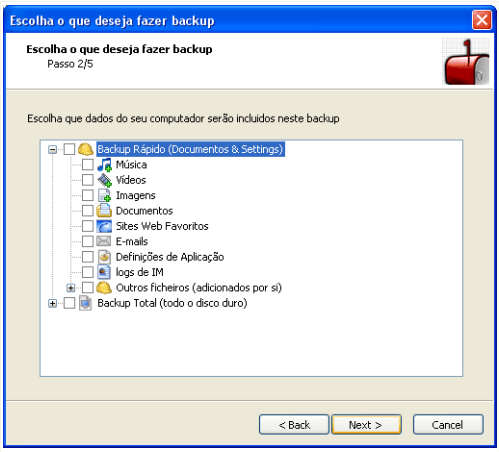

Bem-vindo
Bem-vindo
Bem-vindo ao Assistente do BitDefender Backup.
Este assistente irá ajudá-lo a passar através do processo de criar uma tarefa de backup. No final poderá fazer backup dos seus ficheiros de forma imediata ou agendar o programa para fazer backup dos seus ficheiros mais tarde.
< Back
Next >
Cancel

Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/5 - Escolher do que fazer Backup

Aqui pode escolher que dados do seu computador deseja fazer backup.



Escolher do que fazer backup

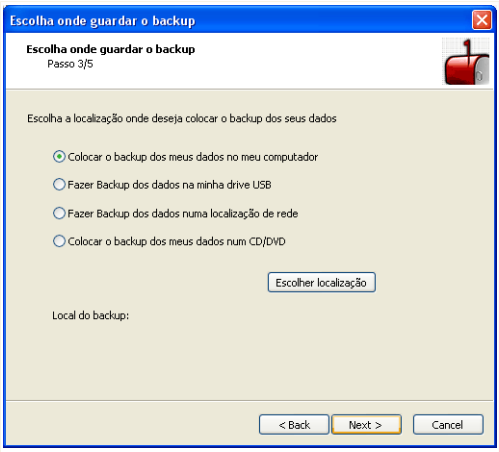
Pode escolher fazer **Backup Rápido** (a sua música, videos, imagens, e-mails, definições de aplicações, etc.) ou **Backup Completo** (todas as partições).

Clique em **Outros ficheiros**, para adicionar outros ficheiros do seu Ambiente de Trabalho ao **Backup Rápido**. O **Backup Completo** pode também ser facilmente personalizado ao seleccionar que directórios de um determinada partição deseja fazer backup.

Clique em **Seguinte**.

Passo 3/5 - Escolher para onde fazer Backup

Aqui pode seleccionar o local onde guardar os dados do backup.


Escolha onde guardar o backup
Escolha onde guardar o backup
Passo 3/5
Escolha a localização onde deseja colocar o backup dos seus dados
Colocar o backup dos meus dados no meu computador
Fazer Backup dos dados na minha drive USB
Fazer Backup dos dados numa localização de rede
Colocar o backup dos meus dados num CD/DVD
Escolher localização
Local do backup:
< Back
Next >
Cancel

Escolha para onde fazer backup

Estão disponíveis as seguintes opções:

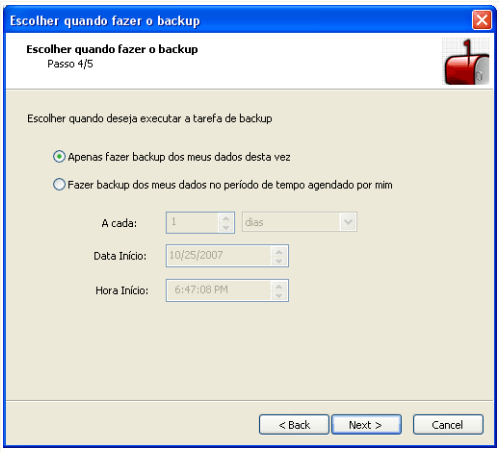
- **Fazer Backup dos meus dados no meu computador**
- **Fazer o Backup para a minha drive USB**
- **Fazer o Backup para um local de rede**
- **Fazer o Backup para o CD/DVD**

Se decidir fazer backup para o seu computador, a sua drive USB ou num local de rede, clique em **Escolher Local** e seleccione o local onde deseja guardar os dados.

Clique em **Seguinte**.

Passo 4/5 - Escolher quando fazer o Backup

Aqui pode seleccionar quando deseja fazer o backup dos dados.



Escolher quando fazer o backup

Estão disponíveis as seguintes opções:

- **Fazer Backup dos dados só esta vez**
- **Fazer Backup dos dados numa data agendada por mim**

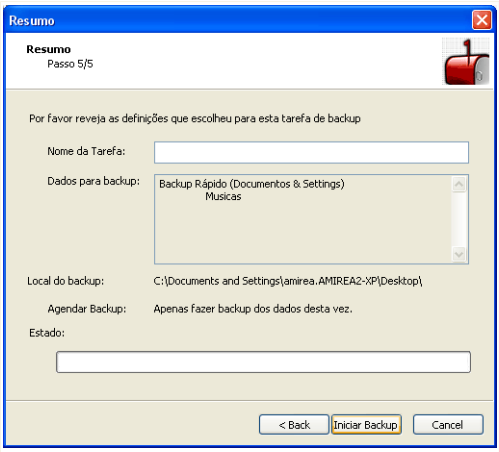
Para fazer backup dos ficheiros na hora clique em **Fazer Backup dos dados só esta vez**, para agendar o produto para fazer backup mais tarde, clique **Fazer Backup dos dados numa data agendada por mim**.

Se seleccionar **Fazer Backup dos dados numa data agendada por mim**, pode especificar com que frequência a tarefa agendada será executada: diariamente ou semanalmente. Pode também especificar a data e a hora.

Clique em **Seguinte**.

Passo 5/5 - Sumário

Aqui pode rever as definições da tarefa de backup.



Resumo

Deve inserir um nome de tarefa no campo correspondente.

Clique em **Iniciar backup** se estiver satisfeito com as suas definições.

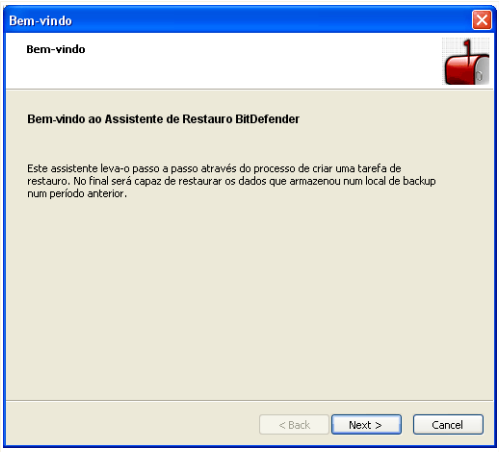
Clique em **Terminar**.

4.2.2. Iniciar Assistente de Restauro

Ao clicar em **Iniciar Assistente de Restauro** um assistente irá levá-lo através do processo de rsetaurar o seu backup.

Passo 1/4 - Janela de Boas-vindas

Esta é uma página de boas-vindas.

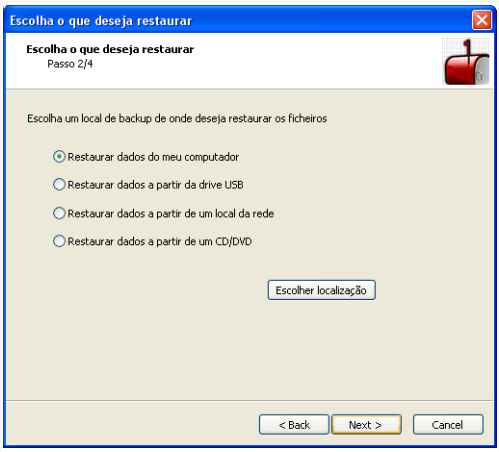

Bem-vindo
Bem-vindo
Bem-vindo ao Assistente de Restauro BitDefender
Este assistente leva-o passo a passo através do processo de criar uma tarefa de restauro. No final será capaz de restaurar os dados que armazenou num local de backup num período anterior.
< Back
Next >
Cancel

Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/4 - Escolha de onde deseja restaurar o Backup

Aqui pode seleccionar um local de onde deseja restaurar os ficheiros.


Escolha o que deseja restaurar
Escolha o que deseja restaurar
Passo 2/4
Escolha um local de backup de onde deseja restaurar os ficheiros
Restaurar dados do meu computador
Restaurar dados a partir da drive USB
Restaurar dados a partir de um local da rede
Restaurar dados a partir de um CD/DVD
Escolher localização
< Back
Next >
Cancel

Escolha de onde deseja restaurar o Backup

Estão disponíveis as seguintes opções:

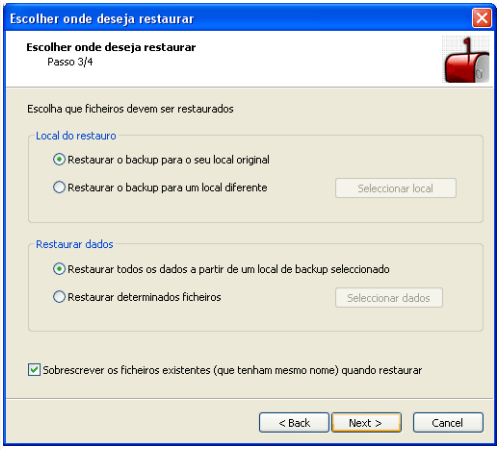
- **Restaurar os dados do meu computador**
- **Restaurar backup de uma drive USB**
- **Restaurar backup de um local de rede**
- **Restaurar backup de um CD/DVD**

Clique em **Escolher Local** e seleccione onde guardar os dados.

Clique em **Seguinte**.

Passo 3/4 - Escolher o Local e os Ficheiros de Restauro

Aqui é onde pode escolher que ficheiros específicos a restaurar e para onde os restaurar.


Escolher onde deseja restaurar
Escolher onde deseja restaurar
Passo 3/4
Escolha que ficheiros devem ser restaurados
Local do restauro
Restaurar o backup para o seu local original
Restaurar o backup para um local diferente
Seleccionar local
Restaurar dados
Restaurar todos os dados a partir de um local de backup seleccionado
Restaurar determinados ficheiros
Seleccionar dados
Sobrescrever os ficheiros existentes (que tenham mesmo nome) quando restaurar
< Back
Next >
Cancel

Escolher o local e os ficheiros de restauro

Estão disponíveis as seguintes opções:

- **Restaurar o backup ao seu local de origem**
- **Restaurar o backup para um local diferente**
- **Restaurar todos os dados do local de backup seleccionado**
- **Restaurar ficheiros específicos**
- **Sobrescrever os ficheiros existentes quando restaurar**

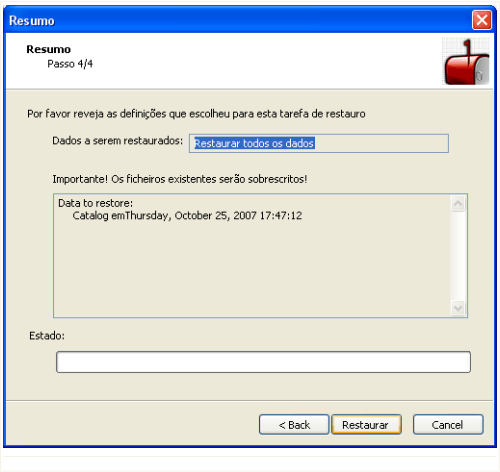
Se deseja restaurar dados para outro local ou apenas ficheiros específicos, seleccione o local e os dados clicando no botão correspondente.

Para evitar sobrescrever o ficheiro esistentes durante o restauro, deseleccione o botão correspondente.

Clique em **Seguinte**.

Passo 4/4 - Sumário

Aqui pode rever as definições da tarefa de restauro.



Clique em **Restaurar** se estiver satisfeito com as suas definições.

Clique em **Terminar**.

4.3. TuneUp

BitDefender vem com um módulo de TuneUp que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco duro.

Para executar operações de manutenção no seu PC, clique na barra **TuneUp** e use as ferramentas disponibilizadas. Estão disponíveis os seguintes botões:

- **Defrag Discos** - inicia o assistente que lhe permite desfragmentar os discos locais.
- **Encontrar Ficheiros Duplicados** - inicia o assistente que lhe permite descobrir e apagar ficheiros em duplicado.
- **Limpar Ficheiros Internet** - inicia o assistente que lhe permite apagar ficheiros temporários da internet e cookies.
- **Destruir Ficheiros** - inicia o assistente que lhe permite remover ficheiros permanentemente do seu computador.
- **Limpar Registo** - inicia o assistente que lhe permite limpar o Registo do Windows.
- **Recuperar Registo** - inicia o assistente que lhe permite recuperar o registo que foi limpo.

4.3.1. Desfragmentar Volumes de Discos Duros

Quando copia um ficheiro que excede o tamanho do maior bloco de espaço livre no disco duro, a fragmentação do ficheiro ocorre. Porque não existe suficiente espaço livre para guardar o ficheiro de forma contínua, o mesmo é armazenado em diversos blocos. Quando o ficheiro framentado é acedido, os seus dados têm de ser lidos de diversos locais diferentes.

A fragmentação dos ficheiros torna mais lento o acesso aos mesmo e diminui o desempenho do sistema. Também acelera o desgaste do seu disco duro.

Para reduzir a fragmentação de ficheiros, deve de desfragmentar os seus discos periodicamente. A desfragmentação do disco reorganiza os dados contidos no disco duro de forma a que as partes constituintes de cada ficheiro sejam armazenadas juntas e de forma continua. Também tenta criar área de espaço livre maiores de forma a evitar que os ficheiros sejam mais tarde fragmentados.

É recomendável que desfragmente o seu disco duro de forma a que:

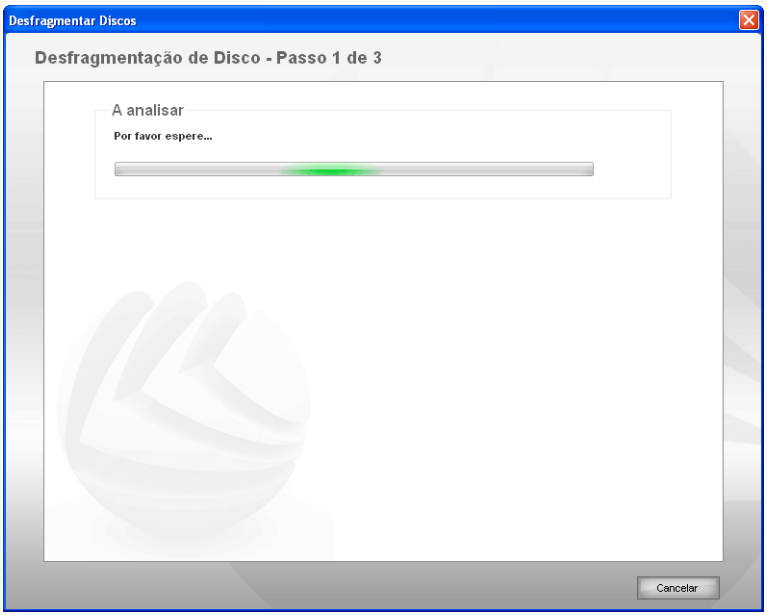
- aceda mais rápido aos ficheiros.
- melhore o desempenho do sistema em geral.
- aumente o tempo de duração do seu disco duro.

Para desfragmentar o disco duro, clique na barra **TuneUp** no Centro de Segurança e depois em **Defrag Discos**. Será de seguida guiado através de um processo completo de três passos.

Nota
A desfragmentação poderá demorar algum tempo uma vez que involve o mover de porções de dados armazenados de um lugar para o outro do disco duro. Recomendamos que execute a desfragmentação quando não está a usar o seu computador.

Passo 1/3 - A analisar...

O Desfragmentador do Disco irá analisar o disco duro para determinar se o mesmo necessita ou não de ser desfragmentado.

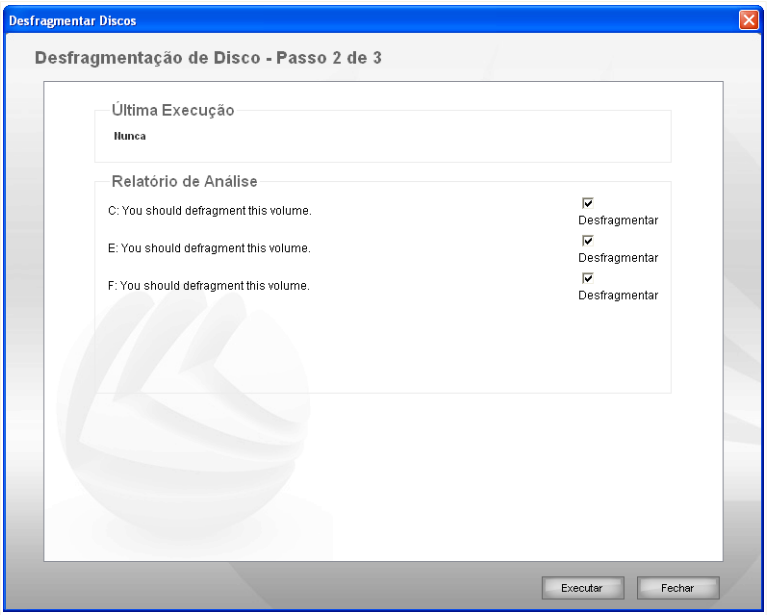


A analisar

Espere que o Desfragmentador do Disco termine a análise.

Passo 2/3 - Ver o Relatório da Análise

Após a análise estar completa, uma nova janela surgirá onde poderá ver os resultados e iniciar a desfragmentação do disco se necessário.



Relatório da Análise

Verifique o relatório da análise.

Se nenhum dos volumes de disco necessita de ser desfragmentado, clique em **Fechar** para fechar a janela. De outra forma, seleccione a opção **Desfragmentar** correspondente aos volumes de disco que necessitam de ser desfragmentados eaclique em **Iniciar** para iniciar a desfragmentação.

Nota

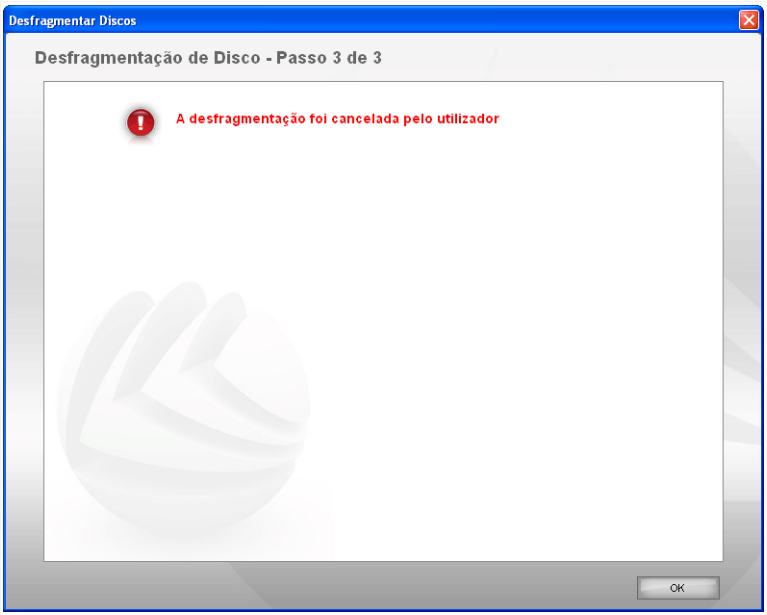
O Desfragmentador do Disco necessita de 15% de espaço livre no disco a desfragmentar de forma a funcionar correctamente. Se não existir suficiente espaço livre no volume a desfragmentar, a desfragmentação será abortada.

Pode cancelar a desfragmentação do disco a qualquer altura clicando em **Abortar**.

Espere que a desfragmentação do disco termine.

Passo 3/3 - Ver Relatório de Desfragmentação

Após a desfragmentação do disco se completar, surgirá uma nova janela onde pode ver as estatísticas de desfragmentação.



Relatório de Desfragmentação

Clique em **OK** para fechar a janela.

4.3.2. Localizar Ficheiros Duplicados

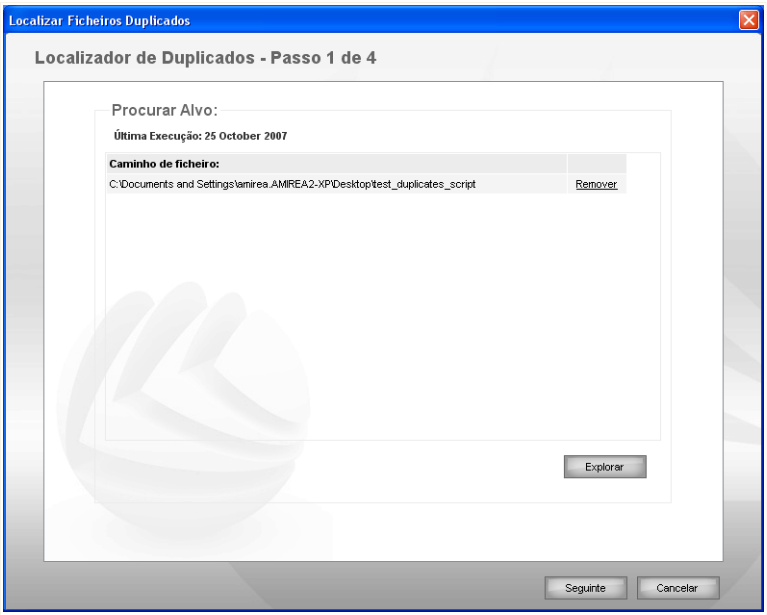
Os ficheiros duplicados comem o seu espaço em disco. Imagine ter o mesmo ficheiro `.mp3` aramazenado em três diferentes locais.

Para detectar e apagar ficheiros duplicados no seu computador, pode usar o Localizador de Duplicados. Desta forma pode melhorar a gestão do espaço livre nos seus discos duros.

Para encontrar duplicados, clique na barra **TuneUp** do Centro de Segurança e depois em **Localizar Ficheiros Duplicados**. Terá de completar um processo guiado de quatro passos.

Passo 1/4 – Seleccionar o Alvo da Procura

Aqui pode especificar onde deseja procurar duplicados.



Alvo da Procura

Clique em **Explorar**, e seleccione o local onde o Localizador de Duplicados deve de procurar por ficheiros duplicados.

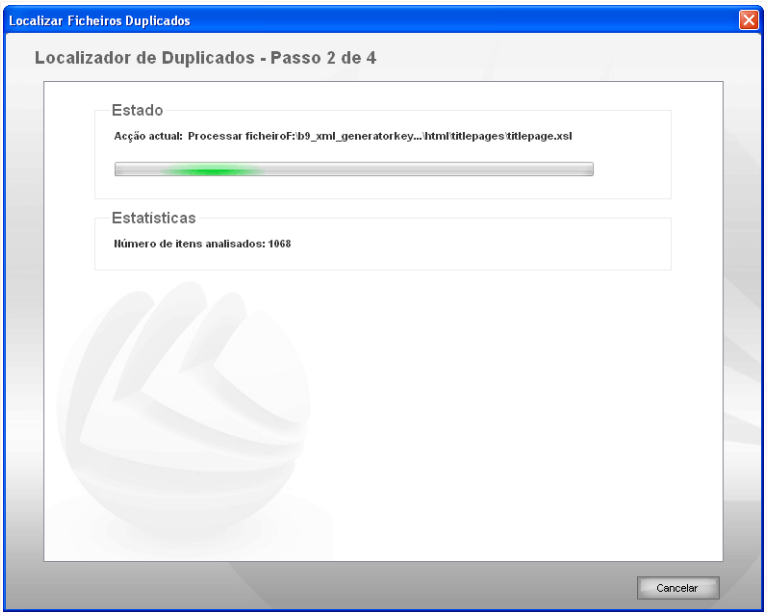
Nota
Pode seleccionar um ou vários locais.

O caminho para o local seleccionado aparecerá na coluna **Caminho Ficheiro**. Se mudar de ideias acerca do local, apenas clique no botão **Remover** ao pé do mesmo.

Clique em **Seguinte**.

Passo 2/4 - A procurar...

O Localizador de Duplicados começará à procura de ficheiros duplicados.



A procurar...

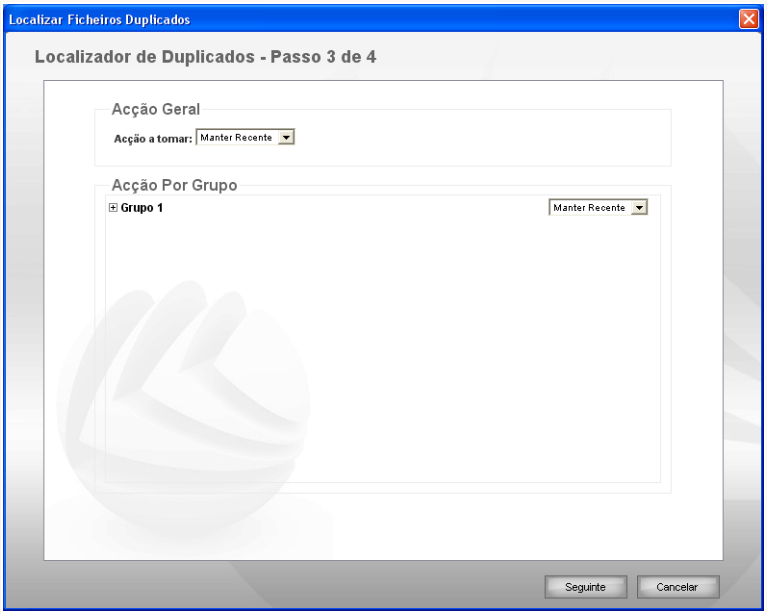
Pode ver o estado da procura e as estatísticas.

Espere que o Localizador de Duplicados complete a sua procura de ficheiros duplicados.

Passo 3/4 - Seleccionar a acção

Após a procura estar terminada, uma nova janela aparecerá onde pode especificar que acções devem ser tomadas sobre os ficheiros duplicados detectados.

Nota
Se não forem encontrados ficheiros duplicados, saltará este passo.



Acções

Pode escolher a acção geral a ser tomada em todos os ficheiros duplicados encontrados ou pode escolher acções a serem tomadas em grupos de ficheiros duplicados.

Estão disponíveis as seguintes acções:

Acção	*Descrição*
Manter Recente	O duplicado mais recente será mantido, enquanto que os outros duplicados serão apagados.
Manter Antigo	O duplicado mais antigo será mantido, enquanto que os outros duplicados serão apagados

Acção	Descrição
Nenhuma Acção	Nenhuma acção será levada a cabo sobre os ficheiros duplicados.

Clique "+" próximo de um grupo para ver os objectos que contém. Se deseja aplicar uma acção geral a todos os objectos de um grupo, seleccione a acção desejada do menu correspondente. Se apena deseja especificar ficheiros do grupo a serem apagados, seleccione a opção **Apagar** ao pé dos respectivos ficheiros.

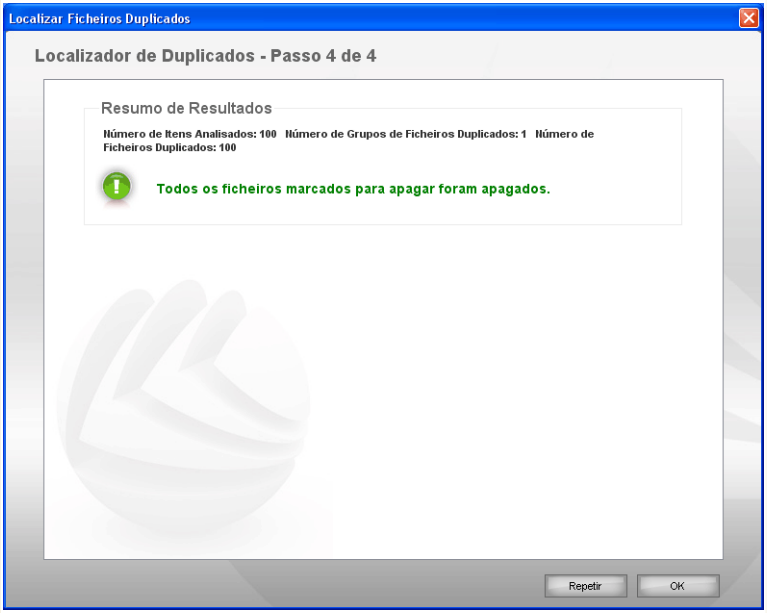
Nota

A acção geral não sobrescreverá a acção escolhida para os ficheiros ou grupos especificados. Isto significa, por exemplo que se define **Manter Recente** como a acção geral, mas escolhe não tomar acção sobre um grupo em particular, então a acção geral será aplicada a todos menos a esse grupo em particular.

Clique em **Seguinte**.

Passo 4/4 - Ver Sumário dos Resultados

Aqui pode ver os resultados da análise do Localizador de Duplicados.


Localizar Ficheiros Duplicados
Localizador de Duplicados - Passo 4 de 4
Resumo de Resultados
Número de Itens Analisados: 100 Número de Grupos de Ficheiros Duplicados: 1 Número de Ficheiros Duplicados: 100
Todos os ficheiros marcados para apagar foram apagados.
Repetir
OK

Sumário dos Resultados

Clique em **Repetir** para iniciar uma nova procura de ficheiros duplicados ou clique em **OK** para fechar a janela.

4.3.3. Limpar Ficheiros da Internet

Cada vez que visita uma página web, são criados ficheiros temporários da Internet de forma a permitir que lhe aceda mais rapidamente da próxima vez.

Apesar de serem apelidados de temporários, estes ficheiros não são apagados quando desliga o seu browser de internet. Isto poderá resultar numa questão de privacidade porque estes ficheiros podem ser vistos por qualquer pessoa que tenha acesso ao seu computador. E mais ainda, estes ficheiros ao fim de algum tempo atingem um tamanho considerável, ocupando desnecessariamente espaço do seu disco duro.

Os cookies também são armazenados na seu computador quando visita uma página web. Os cookies são pequenos ficheiros que contém informação sobre as suas preferências de navegação na web. Eles poderão ser visto também como uma questão

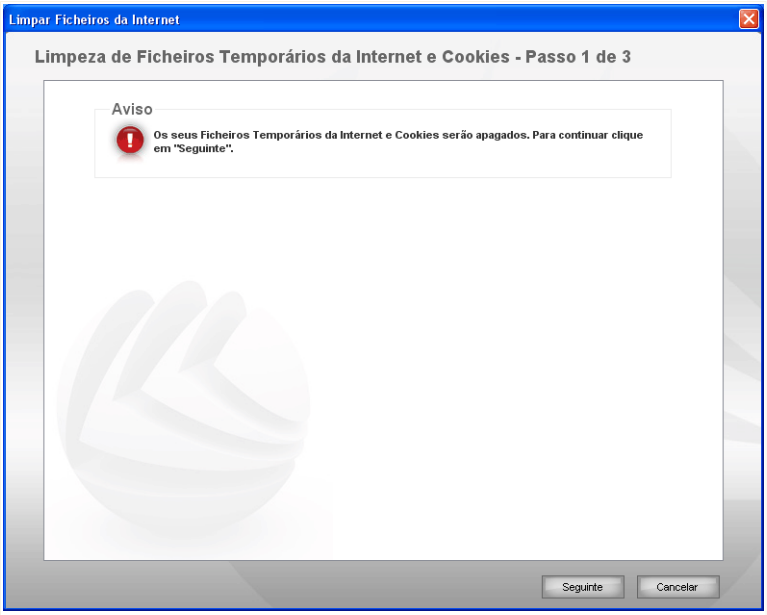
de privacidade também, pois eles podem ser analisados e usados por publicitários para rastrear os seus interesses e gostos on-line.

Ao limpar os seus ficheiros temporários da internet e os cookies, você liberta espaço em disco e protege a sua privacidade.

Para limpar a pasta dos Ficheiros Temporários da Internet, onde o Internet Explorer armazena os ficheiros temporários da internet e os cookies, clique a barra **TuneUp** no Centro de Segurança e depois em **Limpar Ficheiros Internet**. Seguir-se-á um processo guiado de três passos.

Passo 1/3 - Iniciar a Eliminação

Aqui pode dar início à eliminação dos ficheiros temporários da internet e dos cookies.

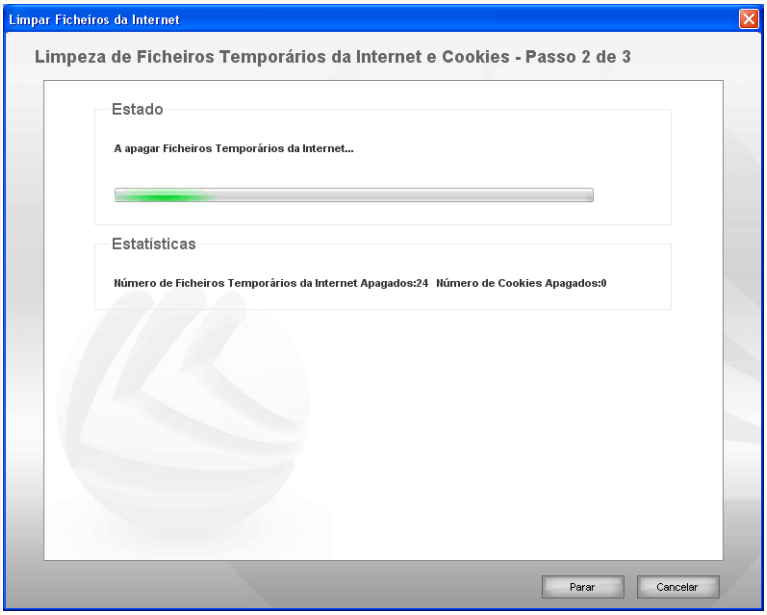

Limpar Ficheiros da Internet
Limpeza de Ficheiros Temporários da Internet e Cookies - Passo 1 de 3
Aviso
Os seus Ficheiros Temporários da Internet e Cookies serão apagados. Para continuar clique em "Seguinte".
Seguinte
Cancelar

Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/3 - A eliminar os ficheiros...

O eliminador começará a apagar os ficheiros temporários da internet e os cookies.

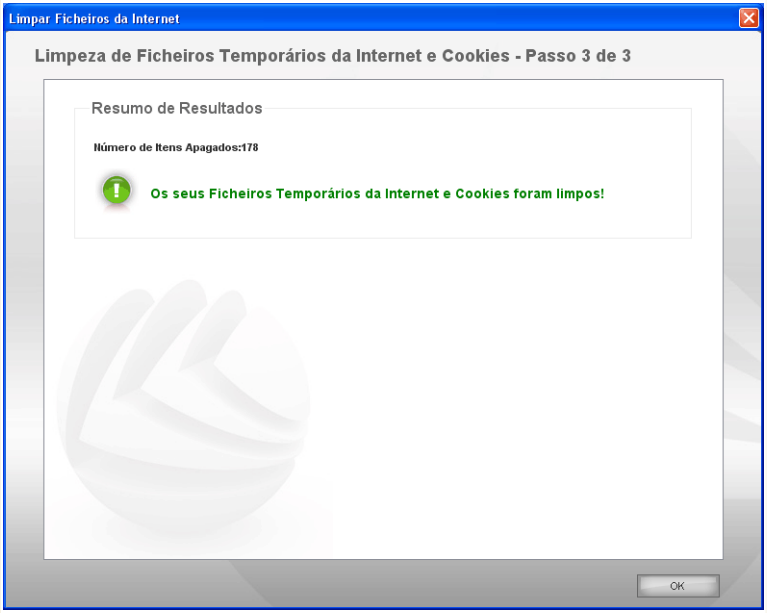

Limpar Ficheiros da Internet
Limpeza de Ficheiros Temporários da Internet e Cookies - Passo 2 de 3
Estado
A apagar Ficheiros Temporários da Internet...
Estatísticas
Número de Ficheiros Temporários da Internet Apagados:24 Número de Cookies Apagados:0
Parar
Cancelar

A eliminar os ficheiros...

Espere que o Eliminador apague os ficheiros temporários da internet e os cookies.

Passo 3/3 - Ver Sumário de Resultados

Após o eliminador ter apagados todos os ficheiros, uma nova janela surgirá onde poderá ver o sumário de resultados.


Limpar Ficheiros da Internet
Limpeza de Ficheiros Temporários da Internet e Cookies - Passo 3 de 3
Resumo de Resultados
Número de Itens Apagados:178
Os seus Ficheiros Temporários da Internet e Cookies foram limpos!
OK

Sumário dos Resultados

Pode ver as estatística com respeitos aos objectos apagados.

Clique em **OK** para fechar a janela.

4.3.4. Apagar Ficheiros Permanentemente

Quando apaga um ficheiro, o mesmo já não fica acessível por meios normais. No entanto o ficheiro continua armazenado no disco duro até que seja sobrescrito quando copiar para lá novos ficheiros.

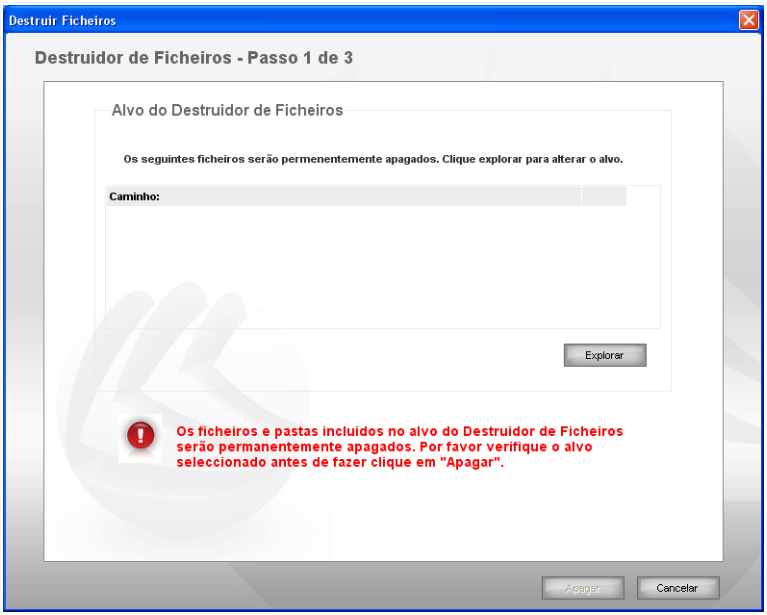
Mesmo que apague o ficheiro, o mesmo pode ser recuperado usando programs especializados. Isto poderá representar uma ameaça à sua privacidade pois poderão ocorrer tentativas maliciosas de se apoderarem da sua informação privada.

Para evitar que informação sensível seja recuperada após a apagar, pode usar o BitDefender para apagar permanentemente aqueles dados removendo-os fisicamente do seu disco duro.

Para apagar permanentemente os ficheiros, clique na barra **TuneUp** do Centro de Segurança e depois em**Destruir Ficheiros**. Depois terá de completar um procedimento guiado de três passos.

Passo 1/3 - Seleccionar Alvo

Aqui pode especificar os ficheiros ou pastas que deseja apagar permanentemente.


Destruir Ficheiros
Destruidor de Ficheiros - Passo 1 de 3
Alvo do Destruidor de Ficheiros
Os seguintes ficheiros serão permenentemente apagados. Clique explorar para alterar o alvo.
Caminho:
Explorar
Os ficheiros e pastas incluidos no alvo do Destruidor de Ficheiros serão permanentemente apagados. Por favor verifique o alvo seleccionado antes de fazer clique em "Apagar".
Apagar
Cancelar

Alvo

Clique em **Explorar**, seleccione o ficheiro ou pasta que deseja apagar e clique em **OK**.

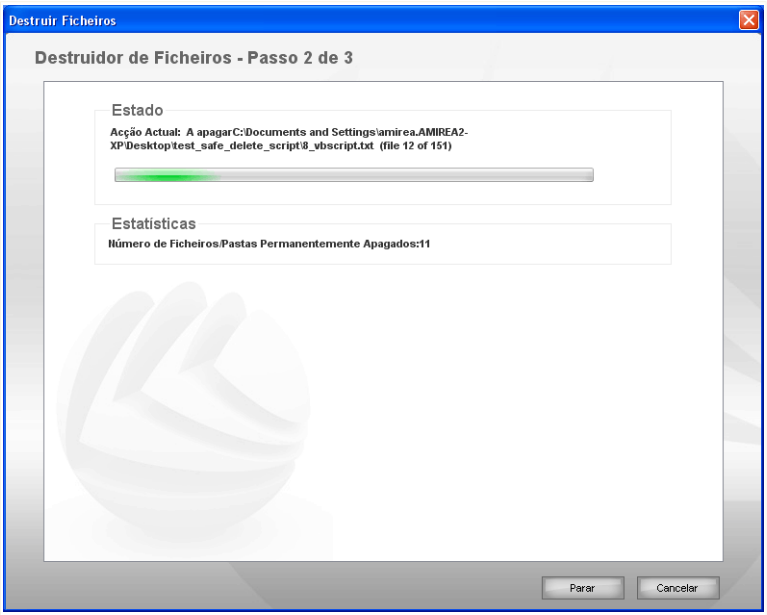
Nota
Pode seleccionar um ou vários locais.

O caminho para o local escolhido aparecerá na tabela. Se mudar de ideias acerca do local, seleccione-o e clqie em **Remover**.

Clique em **Apagar**.

Passo 2/3 - A eliminar os ficheiros...

O BitDefender apagará permanentemente os ficheiros dos locais especificados.

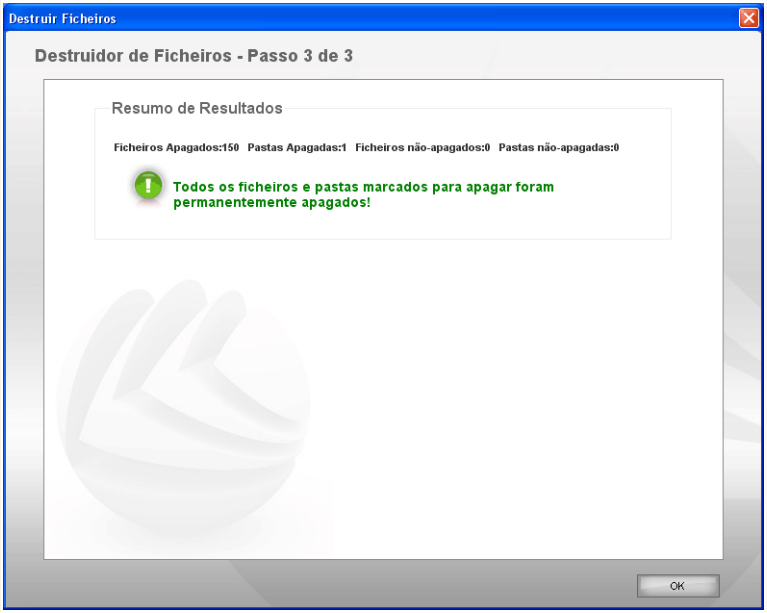


A apagar...

Espere que esta operação termine.

Passo 3/3 - Ver Sumário de Resultados

Após os ficheiros terem sido removidos, uma nova janela aparecerá onde poderá ver os resultados.


Destruir Ficheiros
Destruidor de Ficheiros - Passo 3 de 3
Resumo de Resultados
Ficheiros Apagados:150 Pastas Apagadas:1 Ficheiros não-apagados:0 Pastas não-apagadas:0
Todos os ficheiros e pastas marcados para apagar foram permanentemente apagados!
OK

Sumário dos Resultados

Clique em **OK** para fechar a janela.

4.3.5. Limpar o Registo

O Registo do Windows é uma parte importante dos sistemas operativos baseados no Windows. É uma base de da´dos que contém informação e definições do hardware e do sistema operativo, das aplicações instaladas, utilizadores, preferências do seu computador e outros.

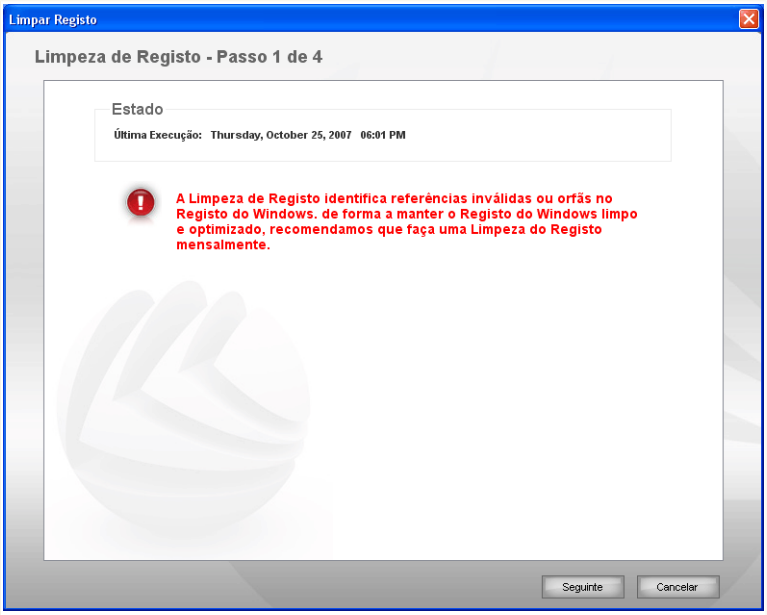
Muitas aplicações escrevem chaves no Registo do Windows durante a instalação. Quando remove tais aplicações, algumas das suas chaves de registo associadas poderão não ser apagadas e continuarem no seu Registo do Windows, tornando o seu sistema mais lento e até causando instabilidade no mesmo. O mesmo acontece quando apaga atalhos para ou determinados ficheiros das aplicações instaladas no seu sistema, como também no caso de drivers corrompidos.

Para limpar o Registo do Windows e melhorar o desempenho do seu sistema, use o Limpa Registo. O Limpa Registo analisa o Registo do Windows e apaga as chaves de registo inválidas.

Para limpar o Registo do Windows, clique na barra **TuneUp** no Centro de Segurança e depois em **Limpar Registo**. Terá de completar de seguida um processo guiado de quatro passos.

Passo 1/4 - Iniciar a Análise

Aqui pode dar início à análise do registo.


Limpar Registo
Limpeza de Registo - Passo 1 de 4
Estado
Última Execução: Thursday, October 25, 2007 06:01 PM
A Limpeza de Registo identifica referências inválidas ou orfãs no Registo do Windows. de forma a manter o Registo do Windows limpo e optimizado, recomendamos que faça uma Limpeza do Registo mensalmente.
Seguinte
Cancelar

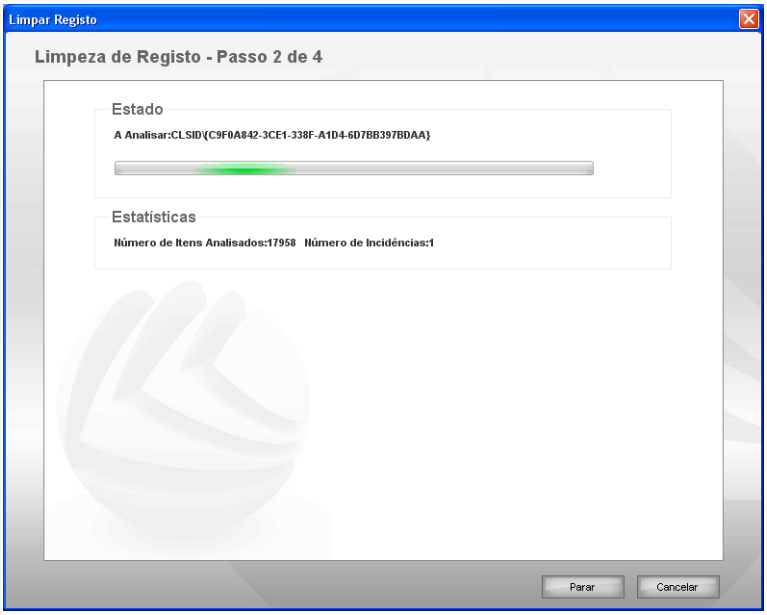
Estado

Pode ver quando o Limpa Registo se executou pela última vez e as recomendações do BitDefender.

Clique em **Seguinte**.

Passo 2/4 - A analisar...

O Limpa Registo começará a analisar o Registo do Windows.



A analisar...

Pode ver a última chave do registo que foi analisada e as estatísticas relacionadas.

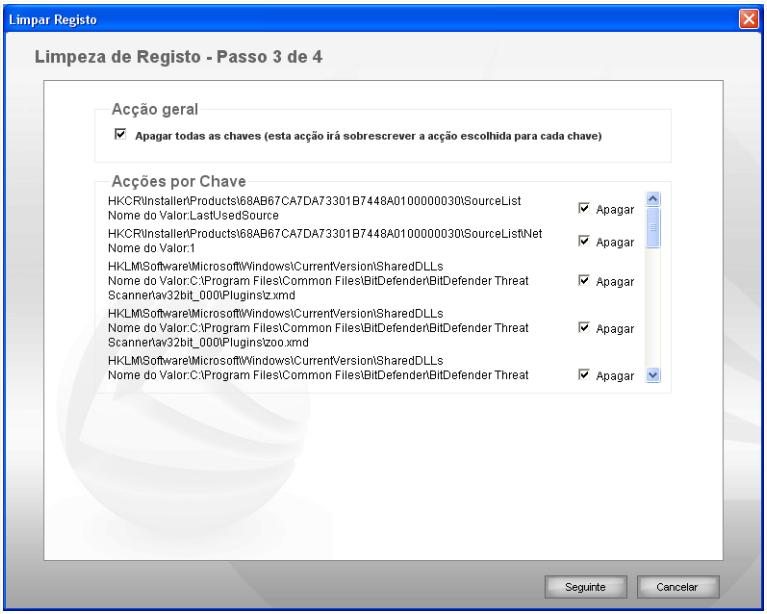
Espere que o Limpa Registo termine a análise do registo.

Nota
Se deseja para a análise, apena clique em **Parar**. Saltará de imediato para o próximo passo.

Passo 3/4 - Seleccionar a acção

Após a análise das chaves do registo estar completa, surgirá uma nova janela onde pode ver os resultados.

Nota
Se não forem encontradas quaisquer incidências ou se escolheu parar a análise, saltará este passo.



Acções

Pode ver todas as chaves de registo detectadas. Pode escolher apagá-las todas ou apenas algumas chaves específicas.

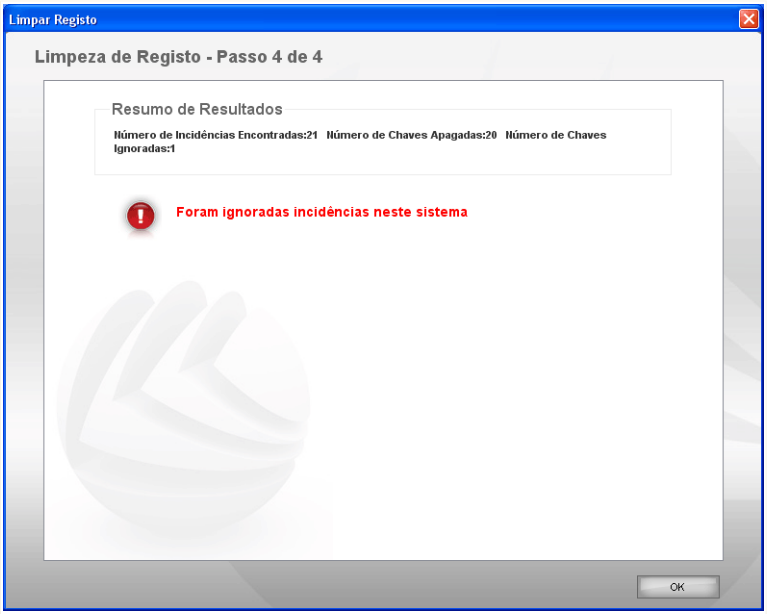
Se seleccionou **Apagar todas**, todas as chaves detectadas serão apagadas. Se deseja eliminar somente chaves específicas, seleccione a opção**Apagar** junto da respectiva chave.

Nota
Por defeito, todas as chaves detectadas serão apagadas.

Clique em **Seguinte**.

Passo 4/4 - Ver Sumário dos Resultados

Aqui poderá ver os resultados da análise executada pelo Limpa Registo.


Limpar Registo
Limpeza de Registo - Passo 4 de 4
Resumo de Resultados
Número de Incidências Encontradas:21 Número de Chaves Apagadas:20 Número de Chaves Ignoradas:1
Foram ignoradas incidências neste sistema
OK

Sumário dos Resultados

Se não escolheu apagar todas as chaves de registo, um texto de aviso será apresentado. Recomendamos que reveja as respectivas incidências.

Clique em **OK** para fechar a janela.

4.3.6. Recuperar Limpeza de Registo

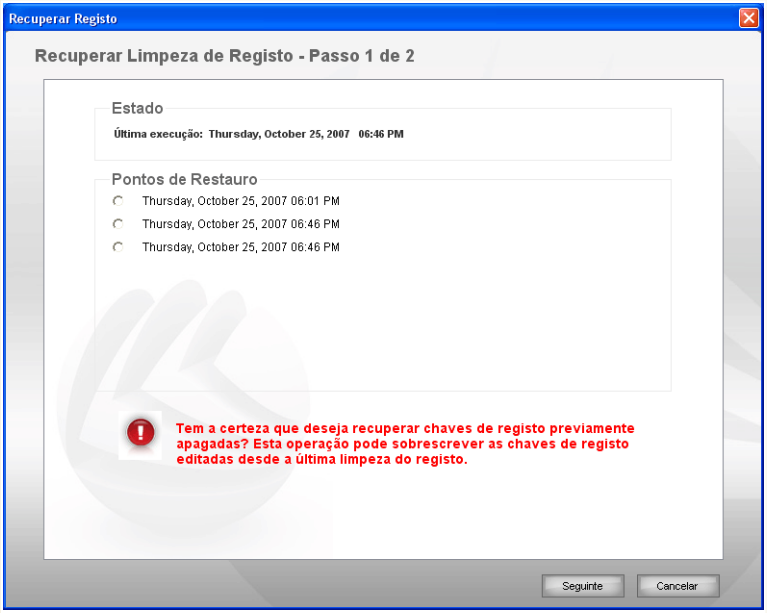
Por vezes, após limparmos o registo, poderá notar que o seu sistema não funciona bem ou que algumas aplicações não funcionam bem devido à falta de chaves no registo. Isto pode ser causado devido a chaves de registo partilhadas que foram apagadas durante a limpeza do registo ou por outras chaves apagadas. Para resolver este problema deverá recuperar o registo que foi limpo.

Para recuperar o registo que foi limpo, clique na barra **TuneUp** do Centro de Segurança e depois em **Recuperar Registo**. Terá de completar de seguida um procedimento guiado com três passos.

Importante
Apenas os utilizadores com direitos de administrador no sistema podem recuperar o registo que foi limpo.

Passo 1/2 - Iniciar Recuperação do Registo

Aqui pode dar início à recuperação da limpeza de registo.


Recuperar Registo
Recuperar Limpeza de Registo - Passo 1 de 2
Estado
Última execução: Thursday, October 25, 2007 06:46 PM
Pontos de Restauro
Thursday, October 25, 2007 06:01 PM
Thursday, October 25, 2007 06:46 PM
Thursday, October 25, 2007 06:46 PM
Tem a certeza que deseja recuperar chaves de registo previamente apagadas? Esta operação pode sobrescrever as chaves de registo editadas desde a última limpeza do registo.
Seguinte
Cancelar

Estado

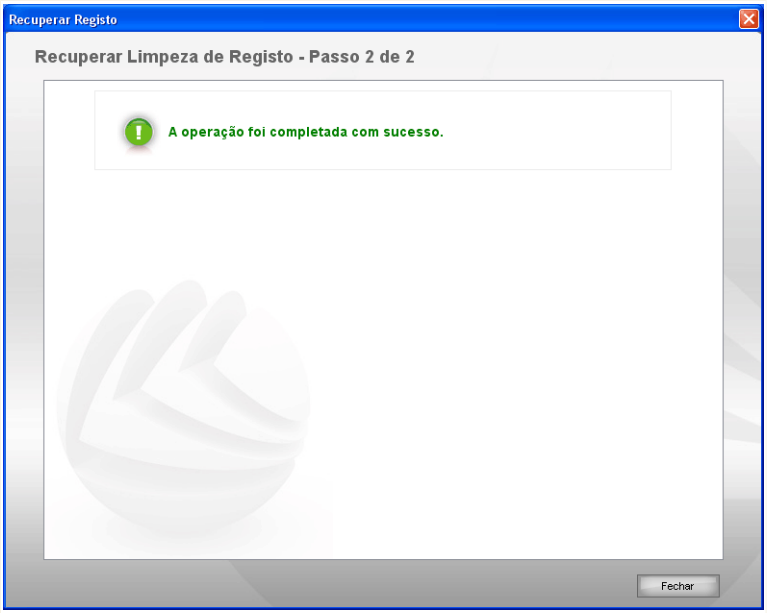
Pode ver quando o Registo do Windows foi limpo pela última vez.

Se tem a certeza que deseja recuperar a chaves de registo que foram apagadas, clique em **Seguinte**.

Atenção
A recuperação da limpeza de registo pode sobrescrever as últimas chaves do registo que foram editadas desde a última limpeza do registo.

Passo 2/2 - Ver Resultados

Aqui pode ver se a recuperação foi bem-sucedida.

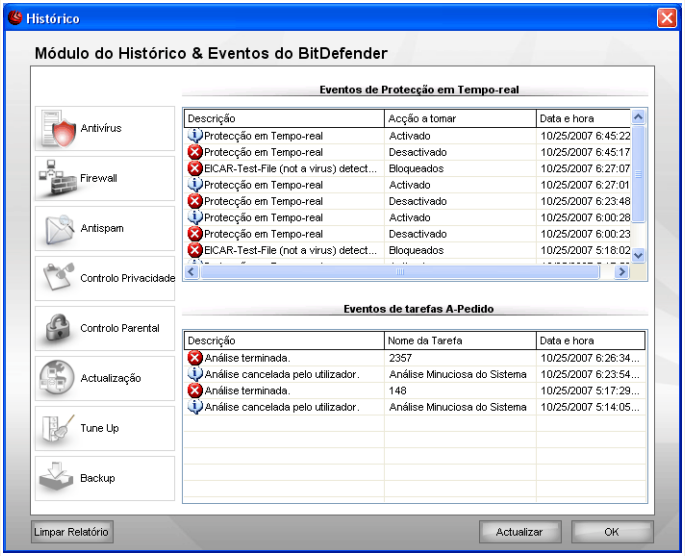


Resultados

Clique em **OK** para fechar a janela.

5. Histórico

O link **Histórico** no fundo da janela do Centro de Segurança BitDefender abre uma outra janela com o histórico & dos eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança. Por exemplo, pode facilmente verificar se a actualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc.



Eventos

De forma a ajudá-lo a filtrar o histórico dos & eventos BitDefender, as seguintes categorias são apresentadas do lado esquerdo:

- **Antivírus**
- **Firewall**
- **Antispam**
- **Controlo Privacidade**
- **Controlo Parental**
- **Tune Up**
- **Backup**

■ **Actualização**

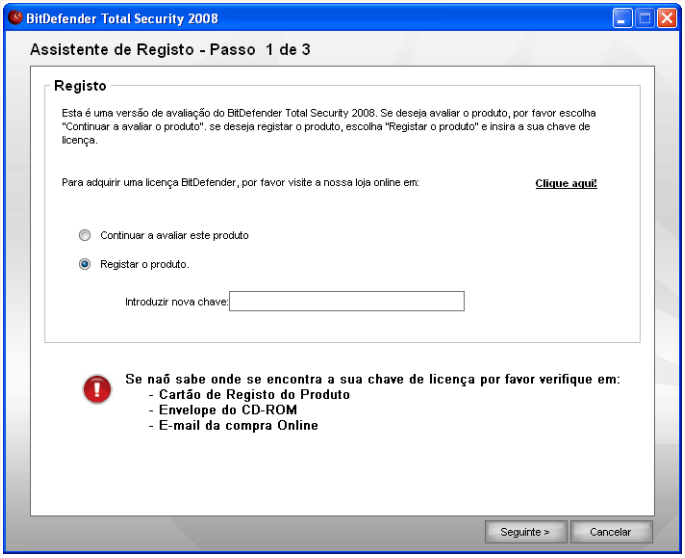
Uma lista de eventos está disponível para cada categoria. Cada evento vem com a seguinte informação: uma breve descripção, a acção que o BitDefender tomou e quando aconteceu, e a data e hora em que ocorreu. Se deseja saber mais informação acerca de um evento em particular da lista, faça duplo clique sobre esse evento.

Clique em **Limpar Log** se deseja remover antigos logs ou **Actualizar** para se certificar que os logs mais recentes são mostrados.

6. Registo

BitDefender Total Security 2008 vem com um período de avaliação de 30 dias. Se dseja registar o BitDefender Total Security 2008, mudar a chave de licença ou criar uma conta BitDefender, clique no link **Registar** , localizado no topo da janela do Centro de Segurança BitDefender. O assistente de registo irá aparecer.

6.1. Passo 1/3 - Registar o BitDefender Total Security 2008


BitDefender Total Security 2008
Assistente de Registo - Passo 1 de 3
Registo
Esta é uma versão de avaliação do BitDefender Total Security 2008. Se deseja avaliar o produto, por favor escolha "Continuar a avaliar o produto". se deseja registar o produto, escolha "Registar o produto" e insira a sua chave de licença.
Para adquirir uma licença BitDefender, por favor visite a nossa loja online em:
Clique aqui!
Continuar a avaliar este produto
Registar o produto.
Introduzir nova chave:
Se naõ sabe onde se encontra a sua chave de licença por favor verifique em:
- Cartão de Registo do Produto
- Envelope do CD-ROM
- E-mail da compra Online
Seguinte >
Cancelar

Registo

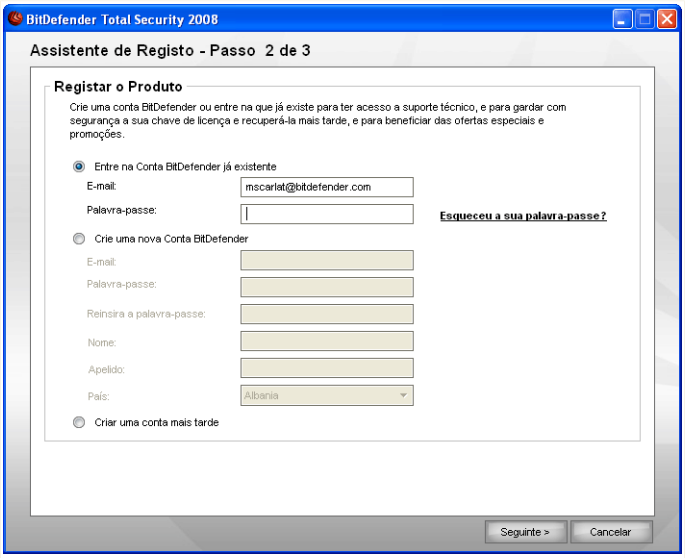
Se não possui uma licença BitDefender, clique no link fornecido para ir para a loja on-line da BitDefender e adquirir uma chave de licença.

Para registar o BitDefender Total Security 2008, seleccione **Registar o produto** e insira a chave de licença no campo **Inserir nova chave**.

Se o período de avaliação ainda não terminou e deseja continuar a avaliar o produto, seleccione **Continuar a avaliar o produto**.

Clique em **Seguinte** para continuar.

6.2. Passo 2/3 - Criar uma conta BitDefender


BitDefender Total Security 2008
Assistente de Registo - Passo 2 de 3
Registar o Produto
Crie uma conta BitDefender ou entre na que já existe para ter acesso a suporte técnico, e para gardar com segurança a sua chave de licença e recuperá-la mais tarde, e para beneficiar das ofertas especiais e promoções.
Entre na Conta BitDefender já existente
E-mail:
mscarlat@bitdefender.com
Palavra-passe:
Esqueceu a sua palavra-passe?
Crie uma nova Conta BitDefender
E-mail:
Palavra-passe:
Reinsira a palavra-passe:
Nome:
Apelido:
País:
Albania
Criar uma conta mais tarde
Seguinte >
Cancelar

Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Nota
Se deseja criar uma conta mais tarde, selecciona a devida opção.

Para criar uma conta BitDefender seleccione**Criar uma nova conta BitDefender** e forneça a devida informação. Os dados que nos fornecer serão mantidos confidenciais.

- **E-mail** - insira o seu endereço de e-mail.
- **Palavra-passe** - introduza uma palavra-passe para a sua conta BitDefender.

> ***Nota***
> A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

- **Reinsira a palavra-passe** - introduza novamente a palavra-passe que previamente definiu.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - seleccione o país em que reside.

> ***Nota***
> Use o endereço de e-mail e a palavra-passe que forneceu para fazer log à sua conta em http://myaccount.bitdefender.com.

Para criar com sucesso uma conta deverá em primeiro lugar activar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para si pelo serviço de registo da BitDefender.

Clique em **Seguinte** para continuar.

Já tenho uma conta BitDefender

BitDefender detectará automaticamente se já possui uma conta BitDefender previamente registada no seu computador. Nesse caso, tudo o que tem de fazer é clicar em **Seguinte**.

Se já possui uma conta activa, mas o BitDefender não a detecta, seleccione**Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a palavra-passe da sua conta.

> ***Nota***
> Se forneceu a palavra-passe incorrecta, será notificado para a re-inserir quando clicar em **Seguinte**. Clique em **OK** para inserir a apalavra-passe novamente ou **Cancelar** para sair do assistente.

Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

Clique em **Seguinte** para continuar.

6.3. Passo 3/3 - Registar o BitDefender Total Security 2008

BitDefender Total Security 2008
Assistente de Registo - Passo 3 de 3
Terminar
Obrigado por usar o BitDefender Total Security 2008. Por favor use o botão Registar da janela principal do produto para obter informação sobre a sua Conta BitDefender e a data de expiração da sua actual chave de licença.
Durante os últimos 30 dias da sua licença BitDefender, o número de dias que faltam para expirar serão mostrados no canto superior esquerdo da janela principal. Para adquirir uma nova chave de licença BitDefender use o botão Comprar disponível na mesma janela.
Abrir a minha Conta BitDefender (requere uma ligação à Internet)
Terminar
Cancelar

Resumo

Seleccione**Abrir a minha conta BitDefender** - para entrar na sua conta BitDefender. Necessita para tal de estar ligado à Internet.

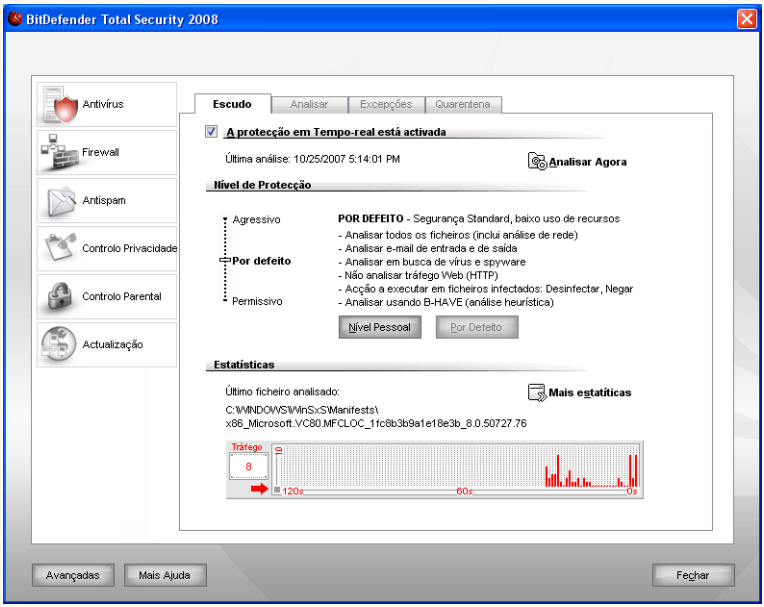
Clique em **Terminar** para fechar a janela.

Administração de Segurança Avançada

7. Consola de Configuração

BitDefender Total Security 2008 vem com uma consola de configuração centralizada, que permite uma administração e configuração avançada do BitDefender.

Para aceder à consola de configuração, clique no link **Configuração** , localizado no fundo do Centro de Segurança.



Consola de Configuração

A consola de configuração está organizada em módulos: **Antivirus**, **Firewall**, **Antispam**, **Controlo Privacidade**, **Controlo Parental** e **Actualização**. Isto permite-lhe gerir facilmente o BitDefender baseado no tipo de incidência de segurança abordada.

Do lado esquerdo da consola de configuração, pode ver o seleccionador de módulos:

- Antivírus - nesta secção pode configurar o módulo do **Antivírus**.
- Firewall - nesta secção pode configurar o módulo da **Firewall**.
- Antispam - nesta secção pode configurar o módulo do **Antispam**.

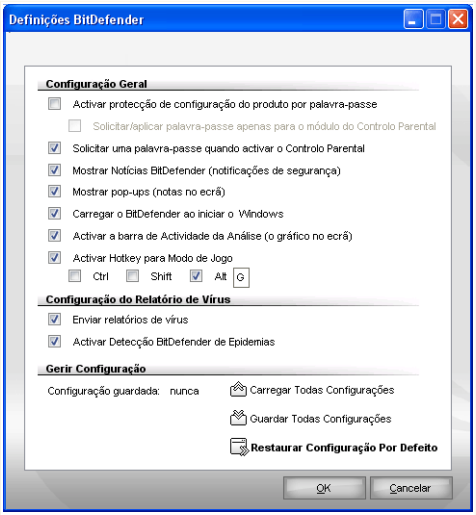
- Controlo de Privacidade - nesta secção pode configurar o módulo do **Controlo Privacidadel**.
- Controlo Parental - nesta secção pode configurar o módulo do **Controlo Parental**.
- Actualização - nesta secção pode configurar o módulo da **Actualização**.

No fundo da consola de configurações, existe um botão de **Mais Ajuda** que abre uma página de ajuda contextual. Clique nesse botão para descobrir mais informação acerca da secção em que se encontra, sempre que necessitar de ajuda adicional.

Se necessita de ajuda adicional, clique no botão **Mais Ajuda**, localizado no fundo da janela. Uma página de ajuda contextual é mostrada e fornece-lhe mais informação detalhada acerca da secção onde se encontra.

7.1. Configurações Gerais

Para configurar as definições gerais do BitDefender Total Security 2008 e gerir as mesmas, clique em **Avançada**. Uma nova janela irá aparecer.


Definições BitDefender
Configuração Geral
Activar protecção de configuração do produto por palavra-passe
Solicitar/aplicar palavra-passe apenas para o módulo do Controlo Parental
Solicitar uma palavra-passe quando activar o Controlo Parental
Mostrar Notícias BitDefender (notificações de segurança)
Mostrar pop-ups (notas no ecrã)
Carregar o BitDefender ao iniciar o Windows
Activar a barra de Actividade da Análise (o gráfico no ecrã)
Activar Hotkey para Modo de Jogo
Ctrl
Shift
Alt
G
Configuração do Relatório de Vírus
Enviar relatórios de vírus
Activar Detecção BitDefender de Epidemias
Gerir Configuração
Configuração guardada: nunca
Carregar Todas Configurações
Guardar Todas Configurações
Restaurar Configuração Por Defeito
OK
Cancelar

Configurações Gerais

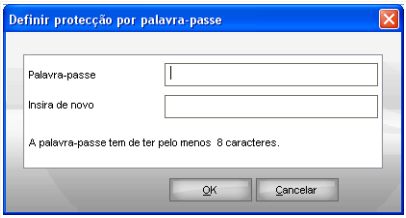
Aqui, pode definir o comportamento geral do BitDefender. Por defeito, o BitDefender é carregado ao iniciar o Windows e é executado minimizado na barra de tarefas.

7.1.1. Configurações Gerais

- **Activar protecção das configurações por palavra-passe** - activa a definição de uma palavra-passe de forma a proteger a configuração do BitDefender.

  Nota
  Se não for a única pessoa a utilizar este computador, recomendamos que protega as suas configurações do BitDefender com uma palavra-passe.

  Se seleccionar esta opção, a seguinte janela aparecerá:



Inserir a palavra-passe

  Introduza a palavra-passe no campo **Palavra-passe**, insira-a novamente no campo **Inserir de novo** e clique em **OK**.

  Uma vez que tenha definido a palavra-passe, será solicitado que a insira sempre que deseje alterar as configurações do BitDefender. Os outros administradores de sistema (se existirem) também terão de inserir a palavra-passe se desejarem alterar as configurações do BitDefender.

  Se desejar ser notificado para inserir a palavra-passe apenas quando configurar o Controlo Parental, deverá também seleccionar **Perguntar/aplicar palavra-passe apenas para o módulo do Controlo Parental**. Por outro lado, se uma palavra-passe for definida apenas para o Controlo Parental e deseleccionar essa opção, a palavra-passe respectiva será requisitada quando configurar qualquer opção do BitDefender.

  Importante
  Se se esqueceu da palavra-passe, terá de reparar o produto para que possa modificar a configuração do BitDefender.

- **Solicitar palavra-passe quando activar o Controlo Parental** - se esta opção estiver activada e nenhuma palavra-passe estiver definida, ser-lhe-á solicitado que a defina quando activar o Controlo Parental.
- **Mostrar Notícias BitDefender (notificações de segurança)** - mostra de tempos em tempos, notificações de segurança relacionadas com epidemias de vírus, enviadas pelo servidor do BitDefender.
- **Mostrar pop-ups (notas no ecrã)** - apresenta uma janela de pop-up no windows que mostra o estado do produto.

- **Carregar o BitDefender ao iniciar o Windows** - executa automaticamente o BitDefender ao iniciar o sistema. Recomendamos que mantenha esta opção seleccionada.
- **Activar a barra de Actividade da Análise (gráfico no ecrã)** - mostra a Barra de Actividade da Análise sempre que entra no Windows. Limpe esta caixa de selecção se não deseja que a Barra de Actividade de Análise seja mostrada.

Nota
Esta opção só pode ser configurada apenas para o actual utilizador do Windows.

- **Activar Hotkey do Modo de Jogo** - permite usar uma combinação de teclas (hotkey) para activar / desactivar o Modo de Jogo. A hotkey por defeito é `Alt+G`.

  para modificar a hotkey, faça o seguinte:

  1. Seleccione as teclas de modificação que deseja usar apartir das seguintes: tecla Control (`Ctrl`), tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
  2. No campo de edição, insira a letra correspondente à tecla que deseja usar.

7.1.2. Configurações do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios de vírus que foram encontrados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a rastrear as epidemias de vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o nome do vírus e será usada, somente para criar relatórios estatísticos.
- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o potencial vírus e será usada somente para ajudar a detectar novos vírus.

7.1.3. Configurações de Administração

Use os botões **Guardar todas as Configurações** / **Carregar todas as Configurações** para guardar/carregar as configurações que tenha feito ao BitDefender

para/de um determinado sítio à sua escolha. Desta forma pode usar as mesmas configurações após reinstalar ou reparar o seu produto BitDefender.

Importante
Apenas os utilizadores com direitos de administrador podem guardar ou carregar configurações.

Para carregar as configurações por defeito, clique em **Restaurar Configurações por Defeito**.

8. Antivírus

BitDefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora).

Para além da análise clássica baseada nas assinaturas do malware, o BitDefender também executa uma análise heurística dos ficheiros. O objectivo da análise heurística é identificar novos vírus, baseado em certos padrões e algoritmos, antes de haver uma nova solução para o vírus. Poderão aparecer falsas mensagens de alarme. Quando é detectado tal programa, este é classificado como suspeito. Nestes casos, recomendamos que envie o ficheiro para análise no laboratório BitDefender.

A protecção que BitDefender oferece está dividida em duas categorias:

- **Análise no-acesso** - previne que novas ameaças de malware entrem no sistema. Isto também é chamado de protecção em tempo-real - os ficheiros são analisados à medida que os usa - no-acesso. Poe exemplo, BitDefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.
- **Análise a-pedido** - permite detectar e remover malware que já se encontra a residir no seu sistema. Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o BitDefender deverá analisar, e o mesmo é analisado – a-pedido. A tarefa de análise permite que crie rotinas personalizadas de análise e elas podem ser agendadas para serem executadas numa base regular.

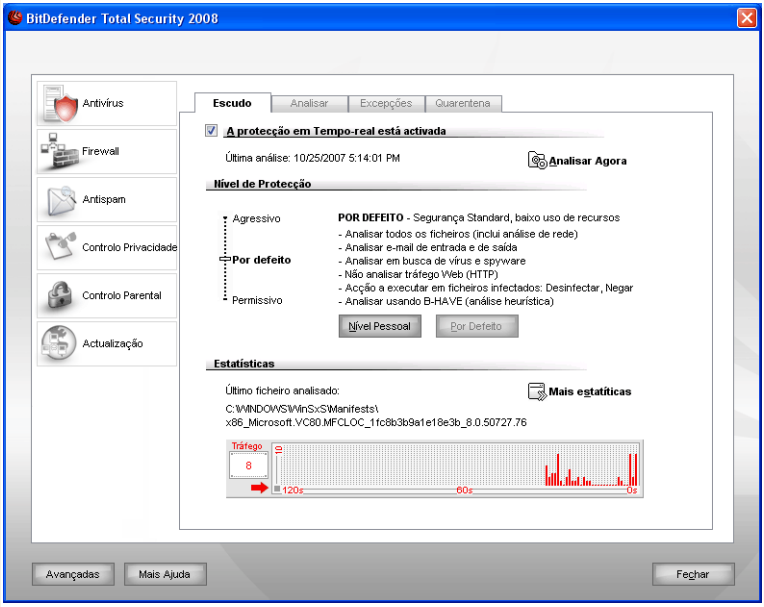
A secção do **Antivírus** deste manual do utilizador contém os seguintes tópicos:

- Análise No-acesso
- Análise A-pedido
- Objectos Excluídos da Análise
- Quarentena

8.1. Análise No-acesso

Analisar ficheiros no -acesso, também conhecida como protecção em tempo-real, mantém o seu computador seguro de todo o tipo de ameaças de malware ao analisar os ficheiros acedidos, e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Para configurar e gerir a protecção em tempo-real clique em **Antivírus>Escudo** na consola de configuração. A seguinte análise irá aparecer:



Protecção em Tempo-real

Importante
Para prevenir que o seu computador seja infectado por vírus mantenha activa a **Protecção em Tempo-real**.

Na parte inferior lateral desta secção pode ver as estatísticas da análise de ficheiros e mensagens de e-mail da **Protecção em Tempo-real**. Clique em **Mais estatísticas** se desejar ver uma janela mais detalhada destas estatísticas.

Pra dar início a uma análise rápida, clique **Analisar Agora**.

8.1.1. Configurar Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de protecção:

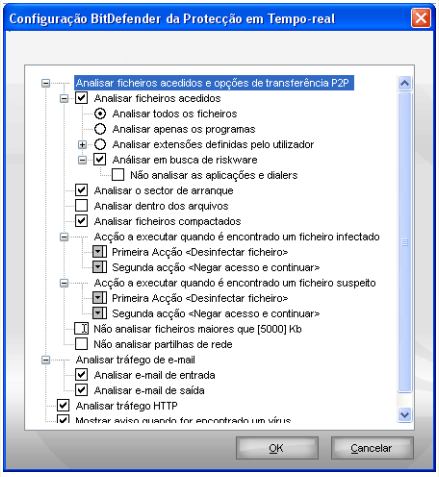
Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Programas e mensagens de e-mail de entrada são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.
Por Defeito	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os ficheiros e mensagens de e-mail de entrada e saída são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os ficheiros, mensagens de e-mail de entrada e saída e tráfego web são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.

Para aplicar as configurações por defeito da protecção em tempo-real clique em **Nível por Defeito**.

8.1.2. Personalizando Nível de Protecção

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Pode personalizar **Protecção em Tempo-real** ao clicar **Nível personalizado**. A seguinte janela aparecerá:



Configurações do Escudo

As opções de análise são organizadas como um menu expansível muito semelhante aos menus usados para explorar o Windows. Clique na caixa com o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

Nota

Pode observar que algumas opções de análise, apesar de terem o sinal "+", não podem ser abertas. Isto acontece porque estas opções ainda não foram seleccionadas. Irá observar que se as seleccionar, elas poderão ser abertas.

- **Analisar ficheiros acedidos e opções de transferências P2P** - examina os ficheiros acedidos e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Mais adiante, seleccione o tipo de ficheiros que pretender examinar.

Opção		Descrição
Analisar ficheiros acedidos	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Apenas os ficheiros de programas serão analisados. Isto significa, apenas os ficheiros com as seguintes extensões: `.exe`; `.bat`;

Opção		Descrição
		.com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Analisar as extensões definidas pelo utilizador	Apenas as extensões especificadas pelo utilizador serão analisadas. Estas extensões têm de estar separadas por ";".
	Analisar em busca de riskware	Analisar em busca de riskware. Os ficheiros detectados serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa. Seleccione **Excluir da análise dialers e aplicações** se deseja excluir este tipo de ficheiros da análise.
Analisar o sector de arranque		Analisa o sector de arranque do sistema.
Analisar dentro dos arquivos		Os arquivos acedidos serão analisados. Com esta opção activa, o computador ficará mais lento.
Analisar ficheiros compactados		Todos os ficheiros compactados serão analisados.
Primeira Acção		Seleccionar do menu drop-down a primeira acção a levar a cabo sobre um ficheiro infectado ou suspeito.
	Negar acesso e continuar	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.
	Limpar Ficheiro	Desinfecta os ficheiros infectados.
	Apagar Ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.

Opção		Descrição
	Mover ficheiro para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial.
Segunda Acção		Seleccionar do menu drop-down a segunda acção a levar a cabo sobre um ficheiro infectado, caso a primeira acção falhe.
	Negar acesso e continuar	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.
	Apagar Ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
	Mover ficheiro para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial.
Não analisar ficheiros maiores do que [x] Kb		Insira o tamanho máximo dos ficheiros a serem analisados. Se o tamanho for 0 Kb, todos os ficheiros serão examinados, independentemente do seu tamanho.
Não analisar partilhas de redes		Se esta opção estiver activada, BitDefender não irá analisar as partilhas de rede, permitindo um acesso de rede mais rápido. Recomendamos que active esta opção aeonas se a rede de que faz parte estiver protegida por uma solução antivírus.

- **Analisar tráfego de e-mail** - analisa o tráfego de e-mail.

  Estão disponíveis as seguintes opções:

Opção	Descrição
Analisar e-mail de entrada	Analisa todas as mensagens de e-mail de entrada.
Analisar e-mail de saída	Analisa todas as mensagens de e-mail de saída.

- **Analisar tráfego HTTP** - Analisa o tráfego HTTP.
- **Mostrar aviso quando for encontrado um vírus** - quando um vírus é encontrado num ficheiro ou numa mensagem de e-mail, irá aparecer uma janela de alerta.

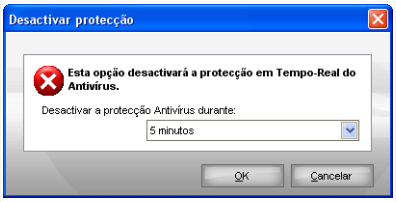
A janela de alerta de um ficheiro infectado, contém o nome e o caminho para o vírus, a acção levada a cabo pelo BitDefender e um link para o site do BitDefender onde poderá encontrar mais informação acerca dele. No caso de um e-mail infectado, a janela de alerta contém também informação acerca do remetente e do destinatário.

Em caso de ser detectado um ficheiro suspeito pode executar um assistente a partir da janela de alerta que o ajudará a enviar esse ficheiro para o Laboratório BitDefender para uma análise mais avançada. Pode inserir o seu endereço de e-mail para receber informação relativa a esse relatório.

Clique em **OK** para guardar as alterações e fechar a janela.

8.1.3. Desactivando a Protecção em Tempo-real

Se deseja desactivar a Protecção em Tempo-real, uma janela de aviso irá aparecer.



Desactivar Protecção em Tempo-real

Deverá confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a sua protecção em tempo-real fique desactivada. Pode desactivar a sua protecção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças do malware.

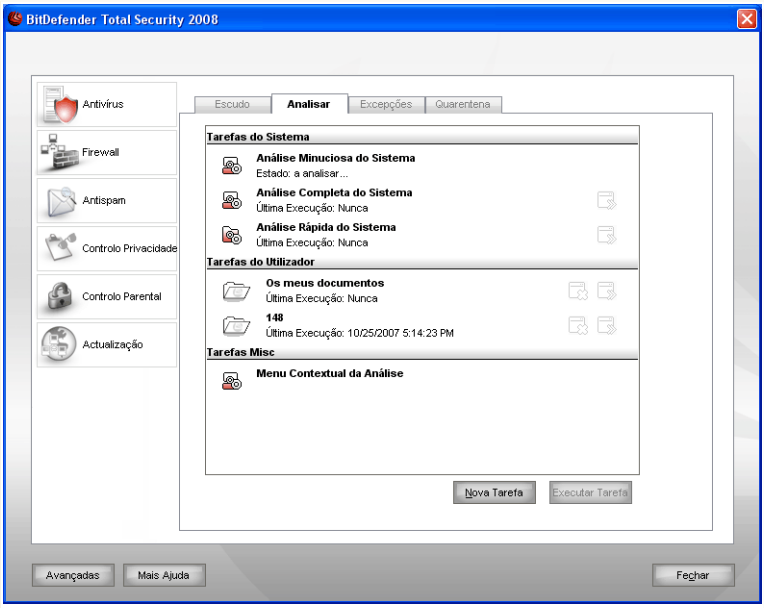
8.2. Análise A-pedido

O objectivo principal do BitDefender é manter o seu computador limpo de vírus. Isto é essencialmente feito ao manter os novos vírus fora do seu computador e ao analisar

as suas mensagens de e-mail e quaisquer novos ficheiros descarregados ou copiados para o seu sistema.

Há o risco de um vírus já se encontrar alojado no seu sistema, mesmo antes de ter instalado o seu BitDefender. Este é o motivo pelo qual é uma excelente ideia analisar o seu computador em busca de vírus residentes depois de instalar o BitDefender. E é definitivamente uma boa ideia, analisar frequentemente o seu computador em busca de vírus.

Para configurar e iniciar uma análise a-pedido, clique **Antivírus>Análise** na consola de configuração. A seguinte análise irá aparecer:



Tarefas de Análise

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados. Pode analisar o computador sempre que desejar ao executar as tarefas de análise por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Pode também agendá-las para que se executem numa base regular ou quando o sistema está sem ser usado de forma a não interferir com o seu trabalho

8.2.1. Tarefas de Análise

O BitDefender vem com diversas tarefas, criadas por defeito, que cobrem as incidências de segurança mais comuns. Pode também criar as suas próprias tarefas personalizadas.

Cada tarefa tem uma janela de **Propriedades** que o permite configurar a tarefa e ver os resultados da análise. Para mais informação, consulte "*Configurar Tarefas de Análise*" (p. 88).

Existem três categorias de tarefas de análise:

- **Tarefas do Sistema** - contém a lista das tarefas por defeito do sistema. As seguintes tarefas estão disponíveis:

Tarefa por Defeito	*Descrição*
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Rápida do Sistema	Analisa as pastas `Windows`, `Programas` e `All Users`. Na configuração por defeito, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.

Nota
Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

- **Tarefas do Utilizador** - contém as tarefas definidas pelo utilizador.

  Uma tarefa chamada `Os Meus Documentos` é fornecida. Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de`

`Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

- **Tarefas Misc** - contém uma lista de tarefas de análise variadas. Estas tarefas de análise dizem respeito a tipos de análise alternativas que não podem ser executadas a partir desta janela. Apenas pode modificar as suas configurações ou ver os relatórios de análise.

Estão disponíveis três botões à direita de cada tarefa:

- **Agendar Tarefas** - indica que a tarefa seleccionada é agendada para mais tarde. Clique neste botão para abrir a janela **Propriedades**, barra Agendador, onde poderá ver a tarefa agendada e modificá-la.
- **Apagar** - remove a tarefa seleccionada.

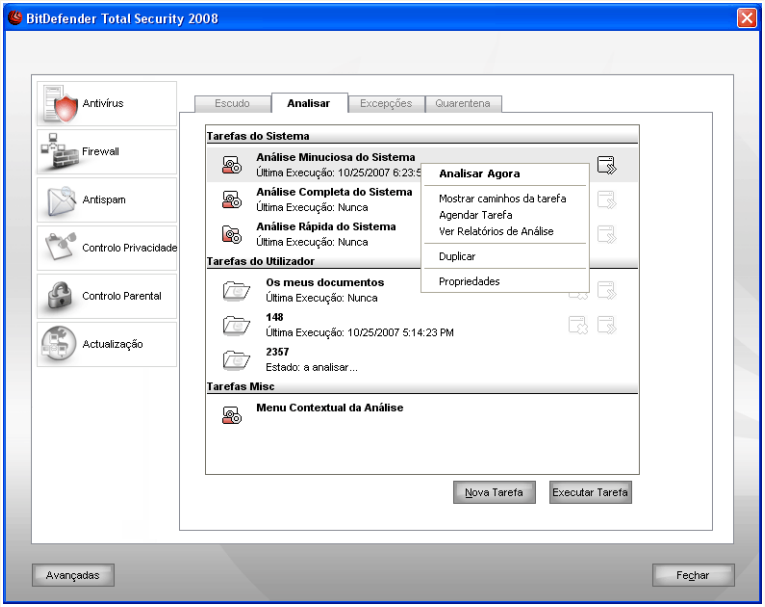
Nota
Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Analisar Agora** - executa a tarefa seleccionada dando início a uma análise imediata.

À esquerda de cada tarefa pode ver o botão**Propriedades**, que o permite configurar a tarefa ou ver os relatórios da análise.

8.2.2. Usando o Menú de Atalho

Um menú de atalho está



Menú de Atalho

disponível para cada tarefa. Clique com o botão direito do rato sobre a tarefa para a abrir.

Os seguintes comandos estão disponíveis no menu de atalho:

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Mudar Alvo da Análise** - abre a janela das**Propriedades**e o botão **Caminho da Análise** , onde pode modificar o alvo da análise para a tarefa seleccionada.

> ***Nota***
> No caso de tarefas do sistema, esta opção é substituida por **Mostrar Caminho Tarefas**, onde apenas poderá ver o alvo da sua análise.

- **Agendar Tarefa** - abre a janela das **Propriedades**e o botão **Agendar**, onde pode agendar a tarefa seleccionada.

- **Ver Relatórios de Análise** - abre a janela das**Propriedades** e a barra**Relatórios de Análise** onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas.
- **Duplicar** - duplica a tarefa seleccionada.

> ***Nota***
> Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.

- **Apagar** - elimina a tarefa seleccionada.

> ***Nota***
> Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Propriedades** - abre a janela das **Propriedades**, e o botão **Geral**, onde pode modificar as configurações para a tarefa seleccionada.

> ***Nota***
> Devido à sua natureza em particular, apenas as opções**Propriedades** e **Ver Relatórios de Análise** estão disponíveis para as tarefas na categoria **Tarefas Misc**.

8.2.3. Criando Tarefas de Análise

Para criar uma tarefa de análise, use um dos seguintes métodos:

- Duplique uma tarefa de análise, renomeia-a e faça as alterações necessárias na janela Propriedades;
- Clique em **Nova Tarefa** para criar uma nova tarefa e configurá-la.

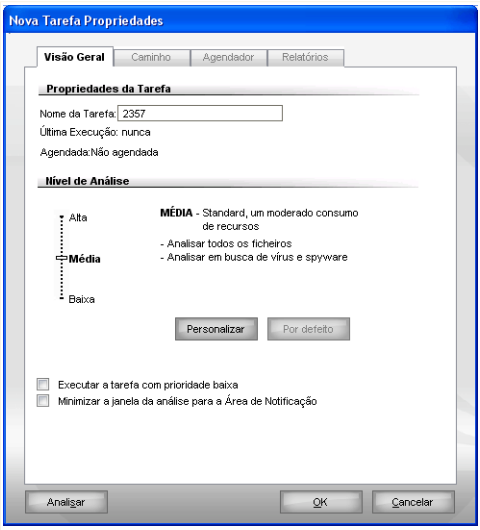
8.2.4. Configurar Tarefas de Análise

Cada tarefa de análise tem as sua própria janela de**Propriedades**, onde pode configurar as opções de análise, definir o alvo da análise, agendar a tarefa ou ver os relatórios. Para abrir esta janela clique no botão **Abrir** , localizado no lado direito da tarefa (ou faça clique-botão direito sobre a tarefa e depois faça clique em **Abrir**).

> ***Nota***
> Para mais informação sobre ver os logs e a barra de **Logs** tab, por favor consulte "*Ver os Relatórios da Análise*" (p. 106).

Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, faça clique-botão direito e seleccione **Propriedades**. A seguinte análise irá aparecer:



Geral

Aqui pode ver a informação acerca da tarefa (nome, a última vez que se executou e o seu estado de agendamento) e definir as configurações da análise.

Escolher Nível de Análise

Pode facilmente configurar a análise ao escolher o nível de análise. Arraste o marcador ao longo da escala para definir o nível de análise apropriada.

Existem 3 níveis de análise:

Nível de Protecção	Descrição
Baixo	Oferece uma eficiência razoável de detecção. O consumo de recursos é baixo.

Nível de Protecção	Descrição
	Programas são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.
Médio	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado. Todos os ficheiros são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.
Elevado	Oferece uma elevada eficiência de detecção. O nível de consumo de recursos é elevado. Todos os ficheiros e arquivos são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada.

Uma série de opções gerais estarão disponíveis para o processo de análise:

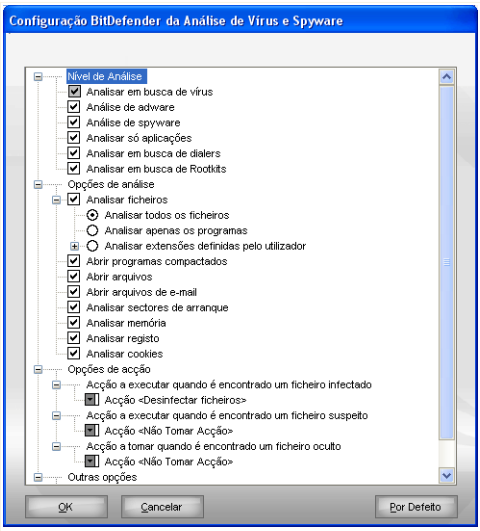
Opção	Descrição
Execute a tarefa de análise com prioridade baixa	Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
Minimizar a janela da análise ao iniciar para a área de notificação	Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Personalizar o Nível de Análise

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Clique em **Personalizar** - para definir as suas próprias opções de análise. Uma nova janela irá aparecer.



Configurações da Análise

As opções de análise são organizadas como um menu expansível muito semelhante aos menus usados para explorar o Windows. Clique na caixa com o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

As opções de verificação estão agrupadas em quatro categorias:

- **Nível de Análise**
- **Opções de análise de vírus**
- **Opções de acção**
- **Outras opções**

- Especifica o tipo de malware que deseja que o BitDefender analise em busca de ao seleccionar determinadas opções da categoria **Nível de Análise**.

  Estão disponíveis as seguintes opções:

Opção	Descrição
Analisar em busca de vírus	Analisa em busca de vírus. O BitDefender também detecta corpos incompletos de vírus, removendo assim qualquer possível ameaça de segurança que possa vir a afectar o seu sistema.
Analisar em busca de adware	Analisa em busca de ameaças de adware. Estes ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.
Analisar em busca de spyware	Analisa em busca de ameaças de spyware. Estes ficheiros serão tratados como ficheiros infectados.
Analisar aplicações	Analisa ficheiros (`.exe` e `.dll` das aplicações).
Analisa em busca de dialers	Procura aplicações de liga~ção para números de valor acrescentado. Estes ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de ligação deste tipo poderá deixar de funcionar se esta opção estiver activa.
Analisar em busca de Rootkits	Analisa em busca de objectos ocultos (ficheiros e processos), conhecidos por rootkits.

- Especifique que tipo de objectos devem ser analisados (ficheiros, mensagens de e-mail e por aí fora) e outras opções. Isto é feito através de seleccionar determinadas opções da categoria **Opções de análise de vírus**.

  Estão disponíveis as seguintes opções:

Opção		Descrição
Análise de ficheiros	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Analisa apenas ficheiros de programa. Isto significa apenas ficheiros com as seguintes extensões: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`;

Opção		Descrição
		chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Analisar as extensões definidas pelo utilizador	Apenas as extensões especificadas pelo utilizador serão analisadas. Estas extensões têm de estar separadas por ";".
Abrir programas compactados		Verifica todos os ficheiros compactados.
Abrir arquivos		Analisa interior dos arquivos.
Abrir arquivos do e-mail		Analisa o interior dos arquivos de e-mail.
Analisar os sectores de arranque		Analisa o sector de arranque do sistema.
Analisar Memória		Analisa a memória em busca de vírus e outro malware.
Analisar registo		Analisa entradas de registo.
Analisar cookies		Analisa os ficheiros cookie.

- Especifique a acção a tomar sobre ficheiros infectados, suspeitos ou ocultos na categoria **Opções de acção**. Pode especificar uma acção diferente para cada categoria.
  - Seleccione a acção a ser tomada sobre o ficheiro infectado. Estão disponíveis as seguintes opções:

Acção	Descrição
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros infectados. Estes ficheiros aparecerão no ficheiro de relatório.
Desinfectar ficheiros	Desinfecta os ficheiros infectados.
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
Mover ficheiros para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial.

  - Seleccionar a acção a tomar sobre um ficheiro suspeito. Estão disponíveis as seguintes opções:

Acção	Descrição
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros suspeitos. Estes ficheiros aparecerão no ficheiro de relatório.
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros suspeitos.
Mover ficheiros para a quarentena	Move os ficheiros suspeitos para a quarentena.

Nota
Há ficheiros suspeitos detectados pela análise heurística. Recomendamos que os envie para o Laboratório do BitDefender.

- Seleccionar a acção a ser tomada sobre os objectos ocultos (rootkits). Estão disponíveis as seguintes opções:

Acção	Descrição
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros ocultos. Estes ficheiros aparecerão no ficheiro de relatório.
Mover ficheiros para a quarentena	Move os ficheiros ocultos para a quarentena.
Tornar visível	Revela ficheiros ocultos de forma a que os possa ver.

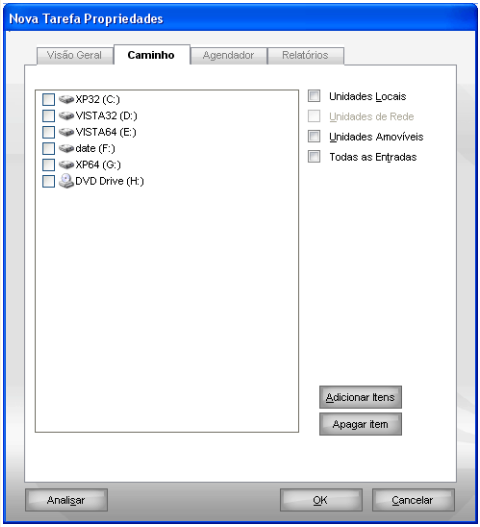
Nota
Se escolher ignorar os ficheiros detectados ou se a acção escolhida falhar, terá de escolher uma acção no assistente de análise.

- Para ser alertado quanto a enviar os ficheiros suspeitos para o Laboratório BitDefender após terminar o processo de análise, seleccione **Enviar ficheiros suspeitos para o Laboratório BitDefender** na categoria **Outras opções**.

Se premir **Defeito** carregará as definições por defeito. Clique em **OK** para guardar as alterações e fechar a janela.

Definir Alvo da Análise

Para definir o alvo da análise de uma tarefa de análise de um utilizador em especial, faça clique com o botão direito do rato sobre a mesma e seleccione **Alterar Alvo da Análise**. A seguinte análise irá aparecer:



Alvo da Análise

Pode ver a lista das drives locais amovíveis e de rede, como também, se houver, os ficheiros e as pastas adicionada previamente. Todos os items seleccionados serão analisados quando a tarefa for executada.

A secção contém os seguintes botões:

- **Adicionar Item** - abre uma janela de exploração, onde pode seleccionar o(s) ficheiro(s) e pasta(s), que pretende analisar.

> ***Nota***
> Pode usar o drag and drop para adicionar ficheiros/pastas à lista.

- **Apagar item** - remove o(s) ficheiro (s) / pasta(s) que foram previamente seleccionados da lista dos objectos a serem analisados.

Nota
Apenas podem ser eliminados o(s) ficheiro(s) / pasta(s) que foram adicionados posteriormente, mas não aqueles que foram automaticamente "enviados" pelo BitDefender.

Para além dos botões explicados acima existem também algumas opções que permitem uma selecção rápida das áreas a analisar.

- **Unidades Locais** - para analisar as drives locais.
- **Unidades de Rede** - para analisar todas as drives de rede.
- **Unidades Amovíveis** - para analisar todas as drives amovíveis (CD-ROM, unidade de disquetes).
- **Todas as Entradas** - para analisar todos as drives, independentemente de serem locais, de rede ou amovíveis.

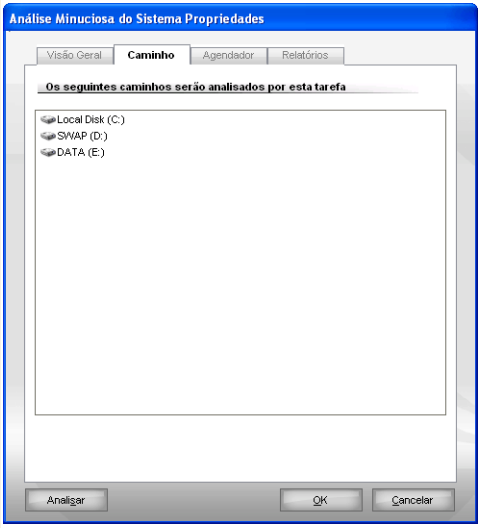
Nota
Se pretende analisar em busca de vírus todo o seu computador, seleccione a caixa de selecção correspondente a **Todas as entradas**.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Ver o Alvo da Análise das Tarefas de Sistema

Não pode modificar os alvos de análise das tarefas de análise a partir da categoria **tarefas do Sistema**. Apenas pode ver o alvo da análise deles.

Para ver o alvo da análise de uma determinada tarefa de análise do sistema, faça clique com o botão direito do rato sobre a tarefa seleccione **Mostrar Caminho da Tarefa**. Por exemplo, para **Análise Completa do Sistema**, a seguinte janela irá aparecer:



Alvo da Análise da Análise Completa do Sistema

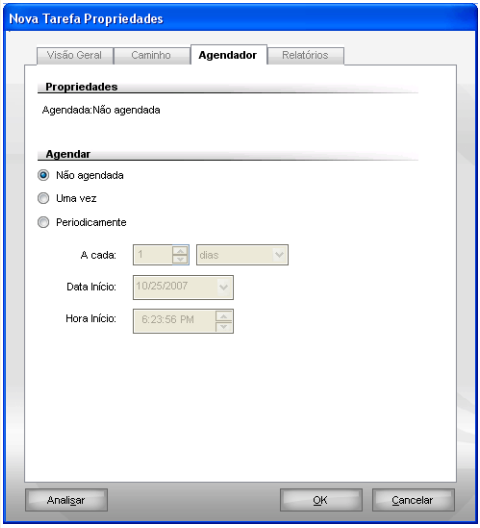
Análise Completa do Sistema e **Análise Minuciosa do Sistema** analisarão todas as drives locais, enquanto **Análise Rápida do Sistema** apenas analisará as pastas `Windows` e `Programas`.

Clique em **OK** para fechar a janela. Para executar uma tarefa, apenas clique em **Analisar**.

Agendar Tarefas de Análise

Com tarefas complexas, o processo de análise leva algum tempo, e funciona melhor se fechar todos os outros programas. É por isso que é melhor agendar tais tarefas para quando não estiver a utilizar o seu computador e este tenha entrado no modo de descanso.

Para ver o agendamento de uma determinada tarefa ou modificá-la, faça clique com o botão direito do rato sobre a tarefa seleccione **Agendar Tarefa**. A seguinte análise irá aparecer:



Agendar

Se houver, pode ver a tarefa agendada.

Quando agendar uma tarefa, deve de escolher uma das seguintes opções:

- **Não agendada** - executa a tarefa apenas quando o utilizador a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - Executa a análise periodicamente, a um determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando numa determinada data e hora.

  Se pretende que a análise seja repetida a um certo intervalo, seleccione a a opção **Periodicamente** e insira na caixa de edição **A cada**, o número de minutos/horas/dias/semanas/meses/anos para indicar a frequência deste processo. Deve de definir a data de início e a hora nos campos**Iniciar Data/Hora**.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

8.2.5. Analisar objectos

Antes de inciar um processo de análise, deveria certificar-se que o BitDefender está actualizado com as assinaturas de malware mais recentes. Analisar o seu computador usando assinaturas desactualizadas pode impedir que o BitDefender detecte novo malware encontrado desde a última actualização. Para verificar quando a última actualização foi feita, clique em **Actualização>Actualização** nas definições da consola.

Nota

Para que o BitDefender possa efectuar uma análise completa, tem de encerrar todos os programas abertos. É especialmente importante que encerre o seu programa de e-mail (por ex. Outlook, Outlook Express ou Eudora).

Métodos de Análise

O BitDefender permite quatro tipos de análise a-pedido:

- Análise imediata - executa uma tarefa de análise das tarefas do sistema/utilizador.
- Análise contextual - faça duplo-clique com o botão direito do rato sobre um ficheiro ou pasta e seleccione BitDefender Antivirus 2008;
- Análise Drag & Drop - Arraste e largue um ficheiro ou pasta em cima da Barra de Actividade da Análise.
- Análise manual - Use a Análise Manual do BitDefender para seleccionar directamente os ficheiros ou pastas a serem analisados.

Análise imediata

Para analisar o seu computador ou parte dele pode usar as tarefas de análise por defeito ou pode criar as suas próprias tarefas de análise. Isto denomina-se análise imediata.

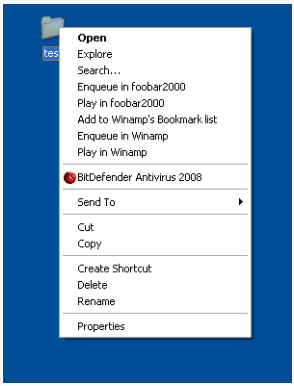
Para executar uma tarefa de análise, use um dos seguintes métodos:

- faça duplo-clique com o rato sobre a tarefa desejada da lista.
- clique no botão **Analisar agora** da correspondente tarefa.
- seleccione a tarefa e depois clique em **Executar Tarefa**.

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 101).

Análise contextual

Para analisar um ficheiro ou pasta, sem configurar uma nova tarefa de análise, pode usar o menu contextual. A isto chamamos de análise contextual.



Análise contextual

Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **BitDefender Antivirus 2008**.

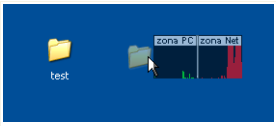
O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 101).

Pode modificar as opções de análise e ver os relatórios ao aceder à janelas das **Propriedades** da tarefa **Análise de Menu Contextual**.

Análise por Drag&Drop

Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

Arraste o ficheiro



Deixe cair o ficheiro

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 101).

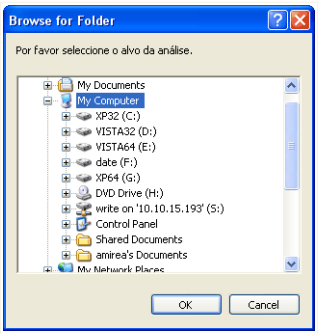
Análise Manual

A análise manual consiste em sleccionar directamente o objecto a ser analisado usando a opção de Análise Manual BitDefender a partir do grupo de programas BitDefender no Menu Iniciar.

Nota
A análise manual é muito útil, pois pode ser executada enquanto o Windows se encontra em Modo de Segurança.

Para seleccionar o objecto a ser analisado por BitDefender, no menu Iniciar do Windows, siga o seguinte caminho **Iniciar** → **Programas** → **BitDefender 2008** → **Análise Manual BitDefender**.

A seguinte análise irá aparecer:



Análise Manual

Escolha o objecto que deseja analisar e clique **OK**.

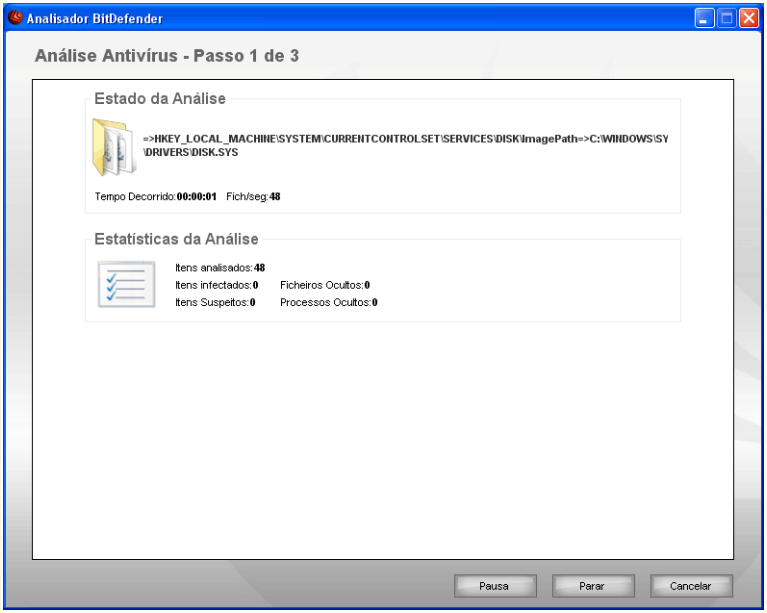
O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte o "*Analisador BitDefender*" (p. 101).

Analisador BitDefender

Quando iniciar o processo de análise a-pedido, o Analisador BitDefender irá surgir. Siga o processo guiado de três passos para completar o processo de análise.

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.



Analisar

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

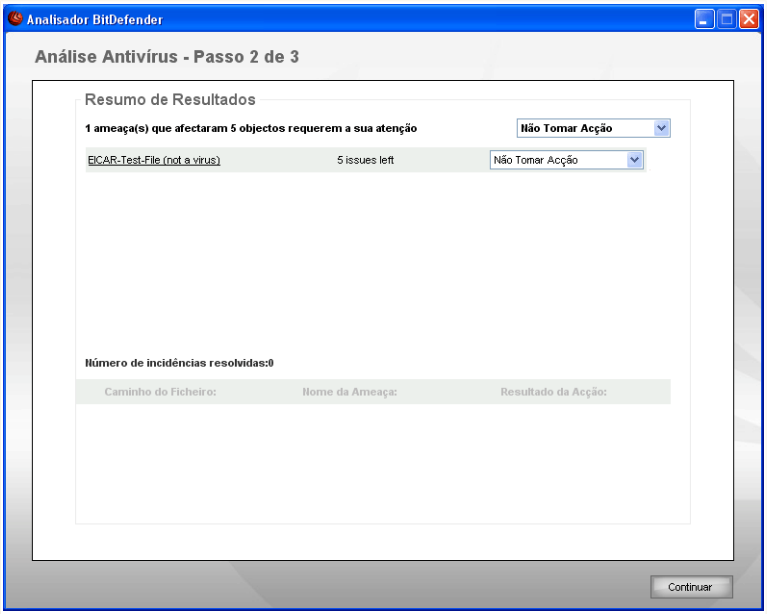
Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá directamente para o último passo do assistente.

Espere que o BitDefender termine a análise.

Passo 2/3 - Seleccionar as acções

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.



Acções

Pode ver o número de incidências que afectam o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Pode escolher uma acção geral a ser tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

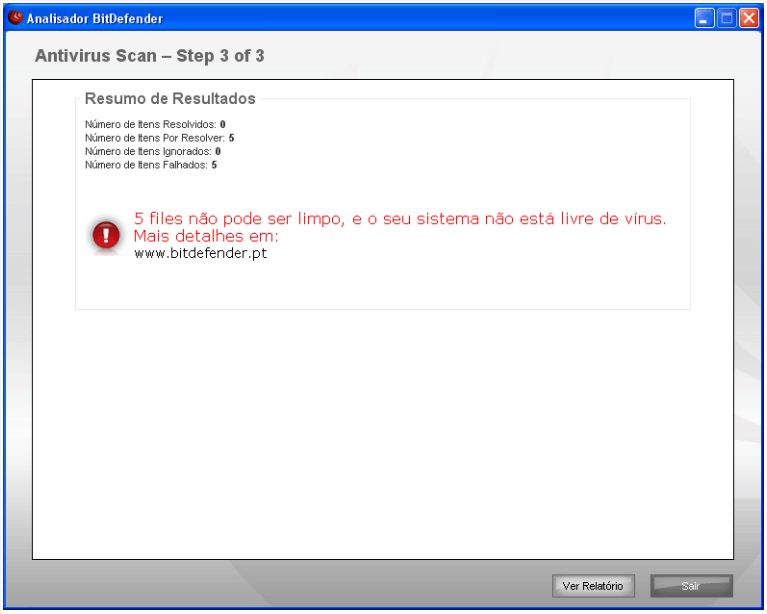
As seguintes opções podem aparecer no menu:

Acção	Descrição
Não Tomar Acção	Nenhuma acção será levada a cabo sobre os ficheiros detectados.
Desinfectar	Desinfecta os ficheiros infectados.
Apagar	Apaga os ficheiros detectados.
Desocultar	Torna visíveis objectos ocultos.

Clique em **Continuar** para aplicar as acções especificadas.

Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.


Analisador BitDefender
Antivirus Scan – Step 3 of 3
Resumo de Resultados
Número de Itens Resolvidos: 0
Número de Itens Por Resolver: 5
Número de Itens Ignorados: 0
Número de Itens Falhados: 5
5 files não pode ser limpo, e o seu sistema não está livre de vírus.
Mais detalhes em:
www.bitdefender.pt
Ver Relatório
Sair

Resumo

Pode ver o resumo dos resultados. O ficheiro do relatório é guardado automaticamente na secção de Logs a partir da janela **Propriedades** da respectiva tarefa.

Importante
Ser-lhe-á solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação.

Clique em **Sair** para fechar a janela.

BitDefender Não pode Resolver Algumas Incidências

Na maioria dos casos BitDefender desinfecta com sucesso os ficheiros infectados ou isola a infecção. No entanto, há incidências que não podem ser resolvidas.

Se existirem incidências não resolvidas, recomendamos que contacte o Suporte Técnico BitDefender em www.bitdefender.pt. O nosso suporte técnico ajuda-lo-á a resover as incidências que está a experimentar.

BitDefender Detectou Itens protegidos por Palavra-passe

A categoria de protegidos por palavra-passe inclui dois tipos de itens: arquivos e instaladores. Eles não representam uma verdadeira ameça à segurança do sistema a não ser que contenham ficheiros infectados e apenas quando são executados.

Para ter a certeza de que estes itens estão limpos:

- Se o item protegido por palavra-passe for um arquivo que protegeu com uma palavra-passe, extraia os ficheiros do mesmo e analise-os separadamente. A forma mais fácil de os analisar é clique botão-direito do rato sobre eles e seleccionar **BitDefender Antivirus 2008** a partir do menu.
- Se o item protegido por palavra-passe for um instalador, certifique-se que a protecção em tempo-real está activa antes de executar esse mesmo instalador. Se o instalador estiver infectado, o BitDefender detectará a situação e isolará a infecção.

Se não deseja que estes objectos sejam detectados novamente pelo BitDefender tem de os adiconar como excepções ao processo de análise. Para adicionar excepções à análise, clique em, **Definições** para abrir a consola das configurações e depois vá para **Antivírus > Excepções** . Para mais informação, consulteObjectos Excluídos da Análise

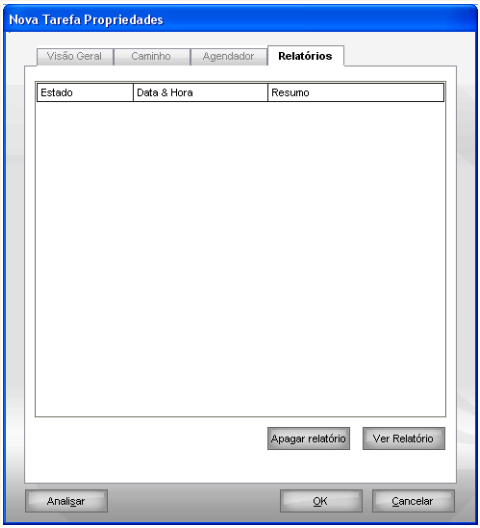
BitDefender Detectou Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

Se foram detectados ficheiros suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender. Clique **OK** para enviar estes ficheiros para uma análise mais avançada no laboratório do BitDefender.

8.2.6. Ver os Relatórios da Análise

Para ver os resultados da análise após a tarefa ter sido executada, faça clique com o botão direito do rato sobre a mesma seleccione **Ver os Relatórios da Análise**. A seguinte análise irá aparecer:



Relatórios da Análise

Aqui pode ver os relatórios gerados cada vez que uma tarefa foi executada.

Cada ficheiro no relatório contém informação sobre o estado do processo de análise registado, a data e hora quando a análise foi feita e um resumo dos resultados da análise.

Estão disponíveis dois botões:

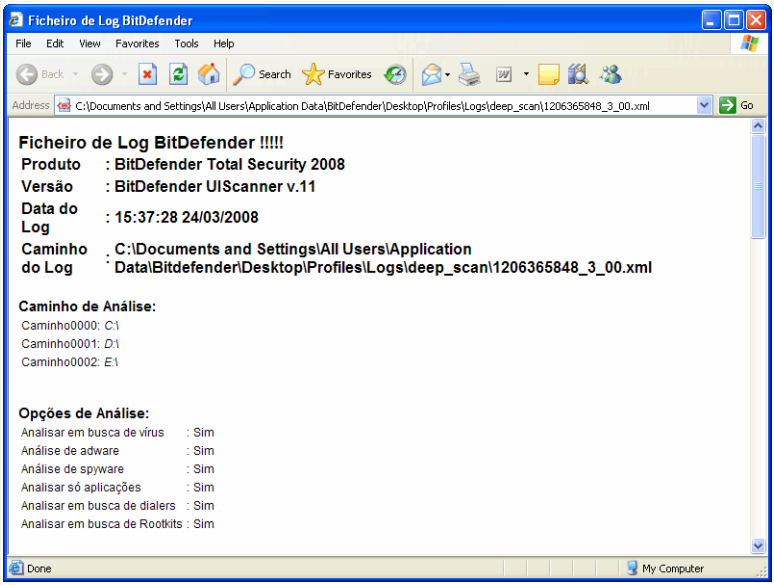
- **Apagar Relatório** - para apagar o relatório seleccionado.
- **Mostrar Relatório** - para ver o relatório seleccionado. O relatório da análise será aberto no seu explorador da internet.

Nota
Também, para ver ou apagar um ficheiro, faça duplo-clique com o rato sobre o ficheiro e seleccione a opção correspondente do menu de atalho.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Exemplo de Relatório da Análise

A seguinte figura representa um exemplo de um relatório de análise:


Ficheiro de Log BitDefender
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\All Users\Application Data\BitDefender\Desktop\Profiles\Logs\deep_scan\1206365848_3_00.xml
Go
Ficheiro de Log BitDefender !!!!!
Produto : BitDefender Total Security 2008
Versão : BitDefender UIScanner v.11
Data do Log : 15:37:28 24/03/2008
Caminho do Log : C:\Documents and Settings\All Users\Application Data\Bitdefender\Desktop\Profiles\Logs\deep_scan\1206365848_3_00.xml
Caminho de Análise:
Caminho0000: C:\
Caminho0001: D:\
Caminho0002: E:\
Opções de Análise:
Analisar em busca de vírus : Sim
Análise de adware : Sim
Análise de spyware : Sim
Analisar só aplicações : Sim
Analisar em busca de dialers : Sim
Analisar em busca de Rootkits : Sim
Done
My Computer

Exemplo de Relatório da Análise

O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

8.3. Objectos a Excluir da Análise

Há casos em que tem de excluir certos ficheiros de serem analisados. Por exemplo, poderá querer excluir um ficheiro de teste EICAR da análise no acesso ou os ficheiros `.avi` da análise a pedido.

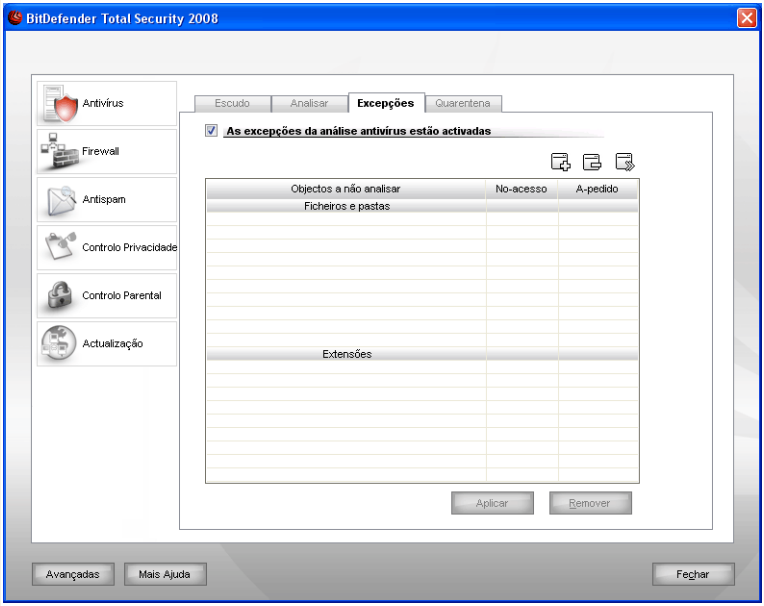
BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

Dois tipos de objectos podem ser excluidos da análise:

- **Caminhos** - o ficheiro ou pasta (incluindo os objectos que contém) indicados por um determinado caminho serão excluídos da análise.
- **Extensões** - todos os ficheiros com um determinada extensão serão excluídos da análise.

Nota
Os objectos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Para ver os objectos excluídos da análise, clique em **Antivírus>Excepções** na consola de configuração. A seguinte análise irá aparecer:



Excepções

Pode ver os objectos (ficheiros, pastas, extensões) que são excluídos da análise. Pode ver por objecto se o mesmo está excluído da análise no-acesso, análise a-pedido, ou ambas.

Nota
As execepções definidas aqui NÃO serão aplicada à análise contextual.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Para editar uma entrada da lista, seleccione-a e clique no botão **Editar**. Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alterção necessárias e clique **OK**.

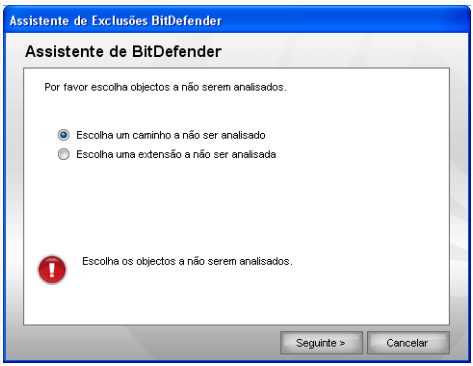
Nota
Pode também clicar no objecto usando o botão direito do rato e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

Clique em **Remover** para reverter as alterações feitas à lista de regras, desde que as mesmas não tenham sido guardadas anteriormente ao clicar **Aplicar**.

8.3.1. Excluir Caminhos da Análise

Para excluir caminhos da análise, clique no botão **Adicionar**. Será guiado através do processo de exclusão de caminhos da análise através de um assistente de configuração que lhe irá aparecer.

Passo 1/3 - Seleccionar o Tipo de Objecto

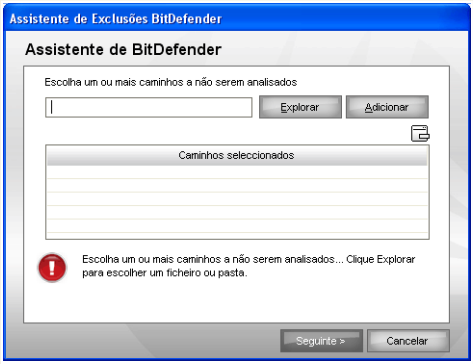

Assistente de Exclusões BitDefender
Assistente de BitDefender
Por favor escolha objectos a não serem analisados.
Escolha um caminho a não ser analisado
Escolha uma extensão a não ser analisada
Escolha os objectos a não serem analisados.
Seguinte >
Cancelar

Tipo de Objecto

Seleccione a opção de excluir um caminho da análise.

Clique em **Seguinte**.

Passo 2/3 - Especificar Os Caminhos a Excluir


Assistente de Exclusões BitDefender
Assistente de BitDefender
Escolha um ou mais caminhos a não serem analisados
Explorar
Adicionar
Caminhos seleccionados
Escolha um ou mais caminhos a não serem analisados... Clique Explorar para escolher um ficheiro ou pasta.
Seguinte >
Cancelar

Caminhos a Excluir

Para especificar os caminhos a excluir da análise use os seguintes métodos:

- Clique em **Explorar**, seleccione o ficheiro ou pasta que deseja excluir da análise e depois clique **Adicionar**.
- Insira o caminho que deseja que seja excluído da análise no campo editado e clique em **Adicionar**.

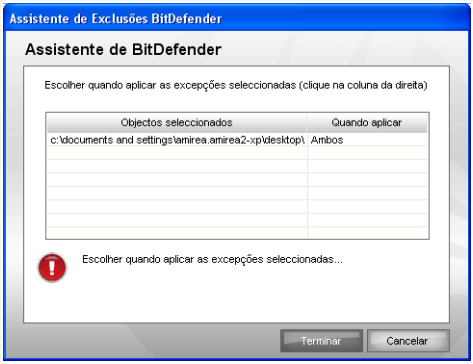
> ***Nota***
> Se o caminho inserido não existe, uma mensagem de erro surgirá. Clique em **OK** e verifique se o caminho é válido ou não.

Os caminhos surgirão na lista à medida que os adicione. Pode adicionar tantos caminhos quanto os que deseje.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Clique em **Seguinte**.

Passo 3/3 - Seleccionar o Tipo de Análise



Tipo de Análise

Pode ver a lista que contém os caminhos a serem excluídos da análise e o tipo de análise do qual eles são excluídos.

Por defeito, os caminhos seleccionados são excluídos da análise no-acesso e a-pedido. Para alterar isto, clique na coluna à direita e seleccione a opção desejada da lista.

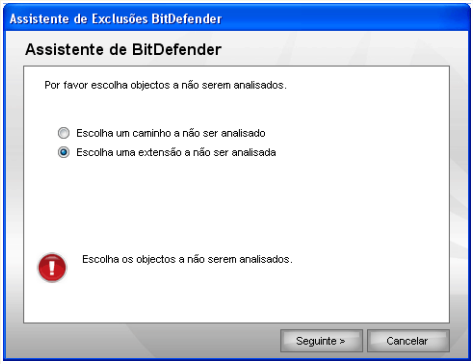
Clique em **Terminar**.

Clique em **Aplicar** para guardar as alterações.

8.3.2. Excluir Extensões da Análise

Para excluir extensões da análise, clique no botão **Adicionar** . Será guiado através do processo de excluir extensões da análise através de um assistente de configuração que irá lhe irá aparecer.

Passo 1/3 - Seleccionar o Tipo de Objecto

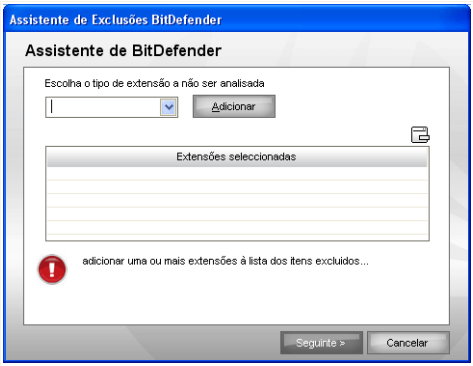

Assistente de Exclusões BitDefender
Assistente de BitDefender
Por favor escolha objectos a não serem analisados.
Escolha um caminho a não ser analisado
Escolha uma extensão a não ser analisada
Escolha os objectos a não serem analisados.
Seguinte >
Cancelar

Tipo de Objecto

Seleccione a opção de excluir uma extensão da análise.

Clique em **Seguinte**.

Passo 2/3 – Especificar Extensões a Excluir


Assistente de Exclusões BitDefender
Assistente de BitDefender
Escolha o tipo de extensão a não ser analisada
Adicionar
Extensões seleccionadas
adicionar uma ou mais extensões à lista dos itens excluidos...
Seguinte >
Cancelar

Extensões a Excluir

Para especificar as extensões a serem excluídas da análise use os seguintes métodos:

- Seleccione a partir do menu a extensão que deseja excluir da análise e clique em **Adicionar**.

> ***Nota***
> O menu contém uma lista de extensões registadas no seu sistema. Quando selecciona uma extensão, pode ver a sua descripção, caso a mesma esteja disponível.

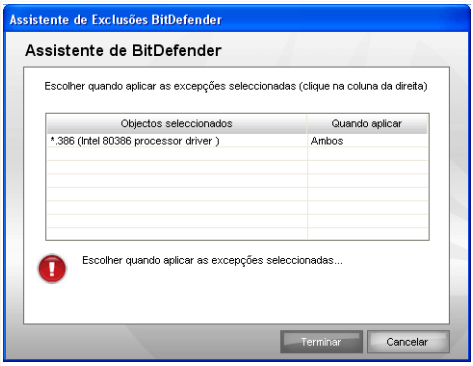
- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

As extensões aparecerão na lista à medida que as adiciona. Pode adicionar tantas extensões quantas as que desejar.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Clique em **Seguinte**.

Passo 3/3 - Seleccionar o Tipo de Análise



Tipo de Análise

Pode ver uma lista contendo as extensões a serem excluídas da análise o o tipo de análise da qual são excluídas.

Por defeito, as extensões seleccionadas são excluidas da análise no-acesso e a-pedido. Para alterar isto, clique na coluna da direita e seleccione a opção que deseja a partir da lista.

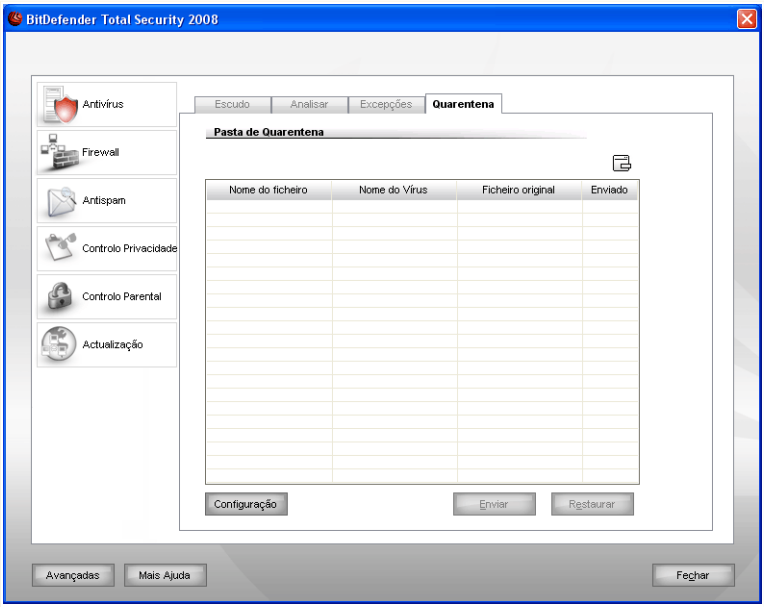
Clique em **Terminar**.

Clique em **Aplicar** para guardar as alterações.

8.4. Àrea de Quarentena

O BitDefender permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Ao isolar estes ficheiros na quarentena, desaparece o risco de infecção,e ao mesmo tempo, terá a possibilidade de enviar estes ficheiros para análise no laboratório do BitDefender.

Para ver e gerir os ficheiros em quarentena e configurar as definições da quarentena, clique em **Antivírus>Quarentena** na consola de configuração.



Quarentena

8.4.1. Gerir Ficheiros em Quarentena

Como pode ver, a secção da **Quarentena** contém uma lista de todos os ficheiros isolados até então. Todo o ficheiro tem incluído o seu nome, tamanho, data de isolamento e de submissão.

Nota
Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não podem ser lidos nem executados.

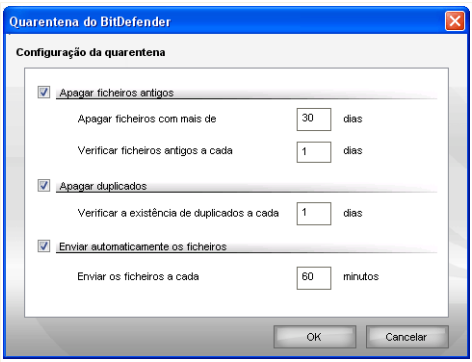
Para apagar um ficheiro seleccionado da lista de quarentena clique no botão **Remover** . Se deseja restaurar o ficheiro seleccionado para a sua localização original clique em **Restaurar**.

Pode enviar qualquer ficheiro seleccionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.

Menu contextual. Está disponível um menu contextual, que lhe permite gerir facilmente os ficheiros em quarentena. As mesmas opções mencionadas previamente estão disponíveis. Pode também seleccionar **Actualizar** para actualizar a secção de Quarentena.

8.4.2. Configuração da Quarantena

Para configurar as definições da quarentena, clique em **Configuração**. Uma nova janela irá aparecer.



Configuração da quarantena

Ao usar a configuração da quarentena, pode definir o BitDefender para executar automaticamente as seguintes acções:

Apagar ficheiros antigos. Para apagar automaticamente ficheiros antigos da quarentena, seleccione a opção correspondente. Deve especificar o número de dias

após os quais os ficheiros em quarentena deverão ser apagados e a frequência com a qual o BitDefender deve de verificar esta situação.

Nota
Por defeito o BitDefender verificará a antiguidade dos ficheiros a cada dia e apagará os que tenham mais de 10 dias de existência.

Apagar duplicados. Para apagar automaticamente ficheiros duplicados na quarentena, seleccione a opção correspondente. Deve especificar o número de dias entre duas verificações consecutivas de duplicados.

Nota
Por defeito, o BitDefender irá verificar ficheiros duplicados na quarentena a cada dia.

Enviar os ficheiros automaticamente. Para enviar automaticamente ficheiros em quarentena, seleccione a opção correspondente. Deve de especificar a frequência com que deseja enviar os ficheiros.

Nota
Por defeito o BitDefender envia automaticamente os ficheiros em quarentena a cada 60 minutos.

Clique em **OK** para guardar as alterações e fechar a janela.

9. Firewall

A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.

Nota
A firewall é essencial se tiver uma ligação de banda larga ou ADSL.

Em Modo Stealth o seu computador fica “escondido” do software maligno e dos hackers. O módulo da firewall é capaz de detectar e proteger automaticamente o seu computador contra os scans de portas (conjunto de pacotes enviados para uma máquina de forma a encontrar "pontos de acesso", frequentemente como modo de preparação para um ataque).

A secção da **Firewall** deste guia do utilizador contém os seguintes tópicos:

- Compreender a Firewall
- Estado da Firewall
- Protecção de Tráfego
- Configuração Avançada
- Actividade da Firewall
- Zonas de Rede

9.1. Compreender a Firewall

A Firewall BitDefender foi desenhada para lhe oferecer a melhor protecção para a sua rede / ligação à Internet, sem ter de a configurar. Não importa se está ligado directamente à Internet, a uma simples rede ou a várias redes (Ethernet, wireless, VPN ou outro tipo de rede), seja fiável ou não-fiável, a firewall irá auto-configurar-se de forma a adaptar-se à situação correspondente.

Por defeito, o BitDefender detecta automaticamente as configurações de rede no seu computador e cria um apropriado perfil básico para a firewall. Também adiciona redes detectadas ao perfil como zonas de rede fiáveis ou não-fiáveis, dependendo da sua configuração.

9.1.1. O que é um Perfil de Firewall?

Um perfil de firewall é um conjunto de regras que controla as aplicações de rede e o acesso à Internet.

Dependendo da configuração de rede do seu computador, o BitDefender cria automaticamente um tipo de perfil específico. O perfil básico criado contém regras de acesso à rede ou regras elementares de acesso à Internet, requeridas pelas aplicações do sistema e pelos componentes BitDefender.

Nota
Um único perfil de firewall é criado, independentemente do número de redes a que esteja ligado.

Existem três tipos básicos de perfis:

Perfil	*Descrição*
Ligação Directa	Contém as regras elementares de acesso à Internet recomendadas para uma configuração de rede que permite um acesso directo à Internet. As regras não permitem que os utilizadores de rede acedam ao seu computador ou que você explore a rede.
Não-Fiável	Contém as regras de acesso à rede recomendadas para uma configuração de rede associada a uma rede não-fiável. A regras permitem-lhe explorar a rede, mas evitam que outros membros de rede acedam ao seu computador.
Fiável	Contém as regras de acesso à rede recomendadas para uma configuração de rede associada a uma rede fiável. Não há restrições impostas no acesso à rede. Isto implica que tem acesso a partilhas de rede, impressoras de rede e outros recursos de rede. Ao mesmo tempo, os membros de rede podem ligar-se ao seu computador e aceder às suas partilhas.

À medida que as aplicações tentam ligar-se à Internet, são adiconadas ao perfil as regras apropriadas. Pode escolher permitir ou negar por defeito o acesso à Internet de aplicações cujas regras não tenham sido configuradas, ou permitir apenas que as

aplicações da lista branca por defeito, e que lhe seja pedida permissão para as restantes aplicações.

Nota

Para especificar a política de acesso das aplicações que tentam ligar-se à Internet pela primeira vez, vá à secção Estado e defina o nível de protecção. Para editar o perfil existente, vá ateá à secção Tráfego e clique em **Editar Perfil**.

9.1.2. O que São Zonas de Rede?

Uma zona de rede representa um computador dentro de uma rede ou uma rede inteira que está completamente isolada do seu computador ou, pelo contrário, que pode detectar o seu computador e ligar-se a ele. Praticamente, uma zona é um endereço IP ou um leque de endereços IP aos quais são permitidos ou negados o acesso ao seu computador.

Por defeito, o BitDefender adiciona automaticamente as zonas para determinadas configurações de rede. A zona é adicionada ao criar uma regra apropriada de acesso à rede, aplicável a toda uma rede, no actual perfil.

Existem dois tipos de zonas:

Tipo de Zona	*Descrição*
Zona Fiável	Computadores de uma zona fiável podem ligar-se ao seu computador e o seu pode ligar-se ao deles. Todas as tentativas de ligação provenientes dessa zona, assim como todas as tentativas de ligação do seu computador a essa zona são permitidas. Se uma rede é adicionada como sendo uma zona segura, você tem livre acesso às partilhas de rede, impressoras de rede e outros recursos de rede. Também os membros da rede podem ligar-se ao seu computador e aceder às suas partilhas.
Zona Não-Fiável	Computadores provenientes de uma zona não-fiável não podem ligar-se ao seu computador e o seu não pode ligar-se ao deles. Todas as tentativas de ligação provenientes dessa zona, assim como todas as tentativas de ligação do seu computador a essa zona são bloqueadas. Como o

Tipo de Zona	Descrição
	tr+afego ICMP é negado e o Modo Stealth está activado, o seu computador é praticamente invísivel para os computadores dessa zona.

Nota

Para editar uma zona, vá até à secção Zonas . Para editar a regra correspondente a uma zona vá até à secção Tráfego e clique em **Editar Perfil**.

9.1.3. Operação da Firewall

Quando reiniciar o sistema após a instalação, o BitDefender automaticamente detectará a sua configuração de rede, e criará um perfil básico apropriado e adicionará uma zona de acordo com a rede detectada.

Nota

Se se liga directamente à Internet, nenhuma zona será criada para a correspondente configuração de rede. Se está ligado a mais do que uma rede, as zonas serão adicionadas dependendo das respectiva redes.

Sempre que uma configuração de rede se altera, quer você se ligue a outra rede ou desactive uma ligação à rede, um novo perfil de firewall é criado. Ao mesmo tempo, as zonas de rede são modificadas de acordo com as alterações.

Quando um novo perfil é criado, o antigo perfil é guardado, de forma a poder ser carregado novamente se você voltar à sua configuração de rede correspondente ao antigo perfil.

Dependendo da configuração de rede, o BitDefender auto-configurar-se-á de acordo com a mesma. Eis como a Firewall BitDefender é configurada por defeito:

- Se se liga directamente à Internet, sem importar se também está ligado a outras redes, um perfil de Ligação Directa é criado. Por outro lado o BitDefender cria um perfil de firewall de rede não-fiável.

  Nota

  Como medida de segurança, perfis fiáveis não são criados por defeito. Para criar um perfil fiável, deve reiniciar o perfil existente. Para mais informação consulte “*Reiniciar Perfis*” (p. 133).

- As zonas são adicionadas dependendo da configuração de rede.

Tipo de Zona	Configuração de Rede
Zona Fiável	**IP Privado sem gateway** - O computador faz parte de uma rede da àrea local (LAN) e não se liga à Internet. Um exemplo disto à uma rede familiar criada para permitir que os membros da família partilhem ficheiros, impressoras e outros recursos.
	IP Privado com Controlador de Domínio detectado - O computador faz parte de uma rede da àrea local (LAN) e está ligado a um domínio. Um exemplo desta situação é uma rede de um escritório que permite que os utilizadores partilhem ficheiros e outros recursos dentro de um domínio. Um domínio implica a existência de um conjunto de políticas as quais os computadores membros seguem.
Zona Não-Fiável	**Wireless Aberta (não segura)** - O computador faz parte de uma rede da área local wireless (WLAN). Um exemplo de tal situação é quando acede à Internet usando um ponto de acesso gratuíto de um lugar público.

Nota

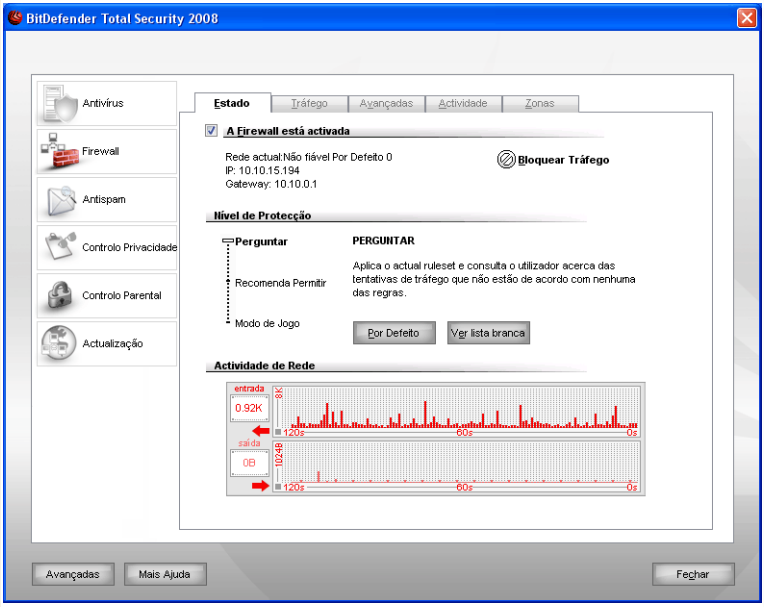
As zonas não são criadas para a mesma configuração de rede, tais como:

- **Pública IP dinâmico** - O computador está directamente ligado à Internet.
- **IP Fixo com gateway, mas sem Controlador de Domínio** - O computador faz parte de uma LAN, sem ser parte de um domínio, e liga-se à Internet através de uma gateway. Um exemplo de uma situação destas é um rede campus de uma escola que permite que os utilizadores partilhem ficheiros e outros recursos.

- O Modo Stealth está activado.
- A VPN e o Acesso Remoto são permitidos.
- O Internet Connection Sharing não é permitido em zonas não-fiáveis.
- As aplicações da lista branca têm automaticamente o acesso permitido, e quanto às restantes aplicações você será solicitado a dar-lhes permissão da primeira vez que elas tentarem ligar-se.

9.2. Estado da Firewall

Para configurar a protecção firewall, clique em **Firewall>Estado** na consola de configuração. A seguinte análise irá aparecer:



Estado da Firewall

Nesta secção pode activar/desactivar a **Firewall**, bloquear todo o tráfego de rede/internet e definir o comportamento por defeito da mesma em novos eventos.

Importante
Para se manter protegido contra os ataques da Internet, mantenha activa a **Firewall**.

Para bloquear toda a rede / Tráfego Internet clique em **Bloquear Tráfego** e depois escolha **Sim** para confirmar a sua opção. Isto irá isolar o seu computador de qualquer outro computador na rede.

Para desbloquer o tráfego mais tarde, basta clicar em **Desbloquear Tráfego**.

Ao fundo e ao lado desta secção pode ver as estatísticas do BitDefender com respeito ao tráfego de entrada e de saída. O gráfico mostra-lhe o volume de tráfego da Internet durante os últimos dois minutos.

Nota
O gráfico aparece mesmo que a **Firewall** esteja desactivada.

9.2.1. Configurar Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

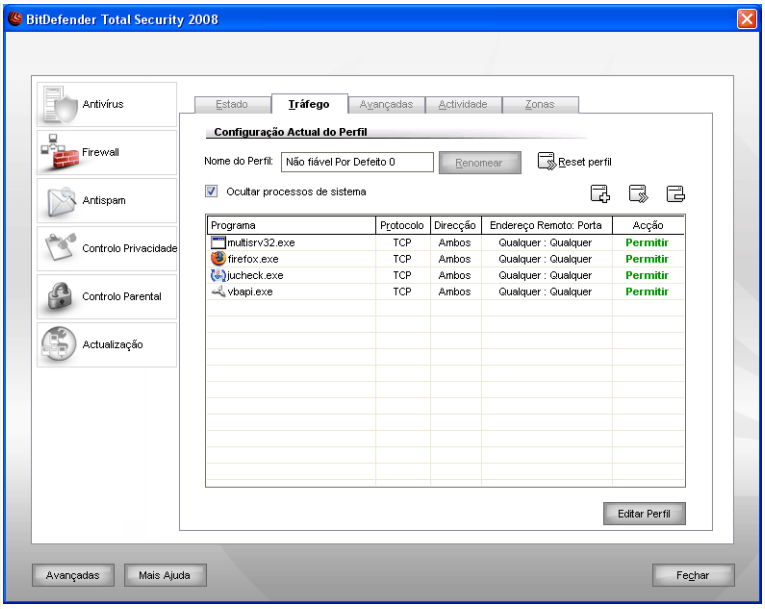
Existem 3 níveis de protecção:

Nível de Protecção	*Descrição*
Modo de Jogo	Aplica as regras actuais e permite as tentativas de tráfego que não correspondem com nenhuma das regras actuais sem o consultar. Esta política é muito desaconselhada, mas poderá ser útil para administradores de redes e jogadores.
Recomenda Permitir	Aplica as regras actuais e permite todas as tentativas de ligação de saída dos programas que BitDefender considera como legítimos (lista branca) sem o consultar. Para as restantes tentativas de ligação, Bitdefender solicitará a sua permissão. Pode ver as regras à medida que são criadas na secção Tráfego. Programas da Lista Branca são as aplicações mais usadas e comuns a nível mundial. Incluem os mais conhecidos browsers de internet, audio&video players, programas de chat e filesharing, como também as aplicações de cliente servidor e do sistema operativo. Se deseja ver quais são os programas da Lista Branca, clique em **Ver Lista Branca**.
Perguntar	Aplica as regras actuais e consulta-o acerca das tentativas de tráfego que não correspondem com nenhuma das regras actuais.

Clique em **Nível por Defeito** para definir a política por defeito(**Recomenda Permitir**).

9.3. Controlo de Tráfego

Para gerir as regras da firewall do actual perfil, clique em **Firewall>Tráfego** na consola de configuração. A seguinte análise irá aparecer:



Controlo de Tráfego

Nesta secção pode definir exactamente quais as ligações de saída e de entrada a permitir/negar, ao criar regras com determinados protocolos, portas, aplicações e/ou endereços remotos.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra).

9.3.1. Adicionar Regras Automaticamente

Com a **Firewall** activada, o BitDefender pedirá a sua permissão sempre que uma tentativa de ligação à Internet seja feita:

Alerta de Firewall BitDefender
vbapi.exe
está a tentar ligar-se à Internet.
Caminho de ficheiro: nents and ... vistext\vbapi.exe
Destino: 1.1.1.1
Protocolo: TCP / Porta: 5700
Este programa está limpo (analisado com o motor Antivírus)
Recomendamos que permita a ligação.
Permitir
Bloquear

Alerta da Firewall

Pode ver o seguinte: a aplicação que se está a tentar ligar à internet, o caminho do ficheiro da aplicação, o destino, o protocolo usado e a porta na qual a aplicação se está a tentar ligar.

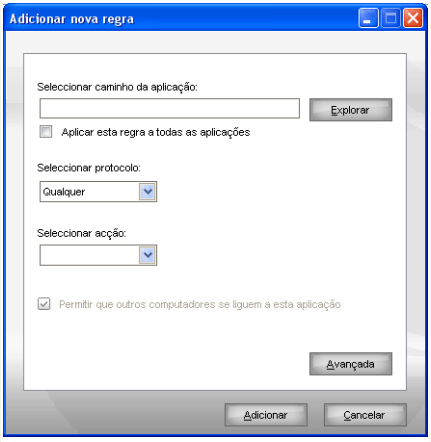
Clique **Permitir** para permitir o tráfego (entrada e saída) gerado por esta aplicação a partir do local host para qualquer destino, no respectivo protocolo IP protocol e em todas as portas. Se clicar em **Bloquear**, será negado completamente o acesso à Internet por parte da aplicação no respectivo protocolo IP.

Baseado na sua resposta, uma regra será criada, aplicada e listada na tabela. A próxima vez que a aplicação se tentar ligar, esta regra será aplicada por defeito.

Importante
Permitir tentativas de ligação de entrada apenas de IP's ou domínios em que confia totalmente.

9.3.2. Adicionar Regras Manualmente

Clique no botão **Adicionar regra** e escolha os parâmetros para a regra. A seguinte análise irá aparecer:



Adicionar Regra

Para adicionar uma nova regra de firewall, siga os seguintes passos:

1. Seleccione aplicação para a qual a nova regra de firewall será criada.

   Para seleccionar a aplicação, clique em **Explorar**, localize-a e clique em **OK**.

   Se deseja criar uma regra para todas as aplicações, apenas seleccione **Aplicar esta regra a todas as aplicações**.
2. Seleccione o protocolo ao qual a regra se aplica.

   Uma lista com os protocolos mais comuns está disponível para o ajudar a seleccionar o protocolo desejado. Seleccione o protocolo desejado (no qual a regra se aplica) a partir do menu drop-down correspondente ou seleccione **Todos** para seleccionar todos os protocolos.

   A seguinte tabela lista os protocolos que pode seleccionar com uma breve descrição de cada um deles:

Protocolo	*Descrição*
ICMP	Internet Control Message Protocol – é uma extensão do Internet Protocol (IP). ICMP suporta pacotes que contêm erro, controlo, e mensagens informativas. O comando de PING, por exemplo, usa o ICMP para testar uma ligação à Internet.

Protocolo	Descrição
TCP	Transmission Control Protocol - TCP permite que dois hosts estabeleçam uma ligação e troquem dados entre si. O TCP garante a entrega dos dados e também garante que os pacotes serão entregues na mesma ordem em que foram enviados.
UDP	User Datagram Protocol - UDP é um meio de transporte baseado em IP desenhado para uma elevada performance. Os jogos e outras aplicações baseadas em vídeo usam com frequência o UDP.

3. Seleccione a acção da regra a partir do menu correspondente.

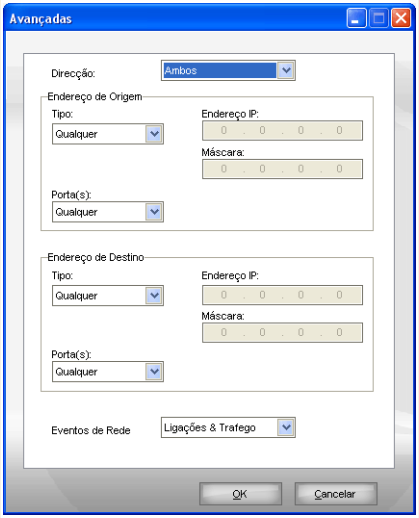
Acção	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

4. Se o protocolo previamente seleccionado é TCP ou UDP, pode especificar se quer ou não que a regra seja aplicada à aplicação quando ela age como servidor.

   Seleccione **Permitir que outros computadores se liguem a esta aplicação** para aplicar a acção a todos os eventos de rede. Implicitamente, você permitirá ou negará a esta aplicação o direito de abrir portas.

   Se deseja aplicar esta acção apenas para tráfego UDP e ligações de tráfego & TCP respectivamente, limpe a correspondente caixa de selecção.

se deseja configurar mais definições avançadas para a regra, clique em **Avançada**. Uma nova janela surgirá:



Configuração Avançada de Regra

Pode configurar o seguinte:

- **Sentido** - selecciona o sentido do tráfego.

Tipo	*Descrição*
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

- **Endereço de Fonte** - especifique o endereço de fonte.

  Para especificar o endereço de fonte, seleccione o tipo de endereço a partir de um menu e especifique a informação requerida. Estão disponíveis as seguintes opções:

Tipo	*Descrição*
Todas	A regra aplica-se a qualquer endereço fonte.

Tipo	Descrição
Host	A regra aplica-se apenas se a fonte for um determinado host. Tem de inserir o IP do host.
Rede	A regra aplica-se apenas se a fonte for uma determinada rede. Tem de inserir o endereço IP e a máscara da rede.
Host Local	A regra aplica-se apenas se a fonte for um host local. Se usa mais do que um interface de rede, selecciona do menu o interface de rede ao qual a regra se aplica. Se deseja que a regra se aplique a todos os hosts locais, seleccione **Todos**.
Rede Local	A regra aplica-se apenas se a fonte for uma rede local. Se está ligado a mais do que uma rede, seleccione do menu a rede à qual a regra se aplica. Se deseja que a regra se aplique a todas as redes locais, seleccione **Todas**.

Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.

- **Endereço de Destino** - especifica o endereço de destino.

Para especificar o endereço de destino, seleccione o tipo de endereço a partir do menu e especifique a informação requerida. Estão disponíveis as seguintes opções:

Tipo	Descrição
Todas	A regra aplica-se a todos os endereços de destino.
Host	A regra aplica-se apenas se o destino é um determinado host. Tem de inserir o IP do host.
Rede	A regra aplica-se apenas se o destino é uma determinada rede. Tem de inserir o endereço IP e a máscara da rede.
Host Local	A regra aplica-se apenas se o destino é o host local. Se usa mais do que um interface de rede, selecciona do menu o interface de rede ao qual a regra se aplica. Se deseja que a regra se aplique a todos os hosts locais, seleccione **Todos**.
Rede Local	A regra aplica-se apenas se o destino é a rede local. Se está ligado a mais do que uma rede, seleccione do menu a rede à qual a regra se aplica. Se deseja que a regra se aplique a todas as redes locais, seleccione **Todas**.

Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.

- **Eventos de Rede** - se escolheu o TCP ou o UDP como protocolo, escolha os eventos de rede aos quais a regra se aplica.

Clique em **OK** para fechar a janela de configuração avançada.

Clique em **Adicionar** para adicionar a regra de firewall.

9.3.3. Gerir Regras

Pode ver na tabela as regras criadas até agora para o actual perfil.

Seleccione a caixa de selecção correspondente a **Ocultar processos de sistema** para esconder as regras que dizem respeito aos processos de sistema e do BitDefender.

As regras são listadas em ordem de prioridade começando no topo, com a primeira regra com a maior prioridade. Clique em **Editar perfil**para entrar no ecrã **Visão Detalhada** onde pode mudar a prioridade das regras movendo-as para cima ou para baixo.

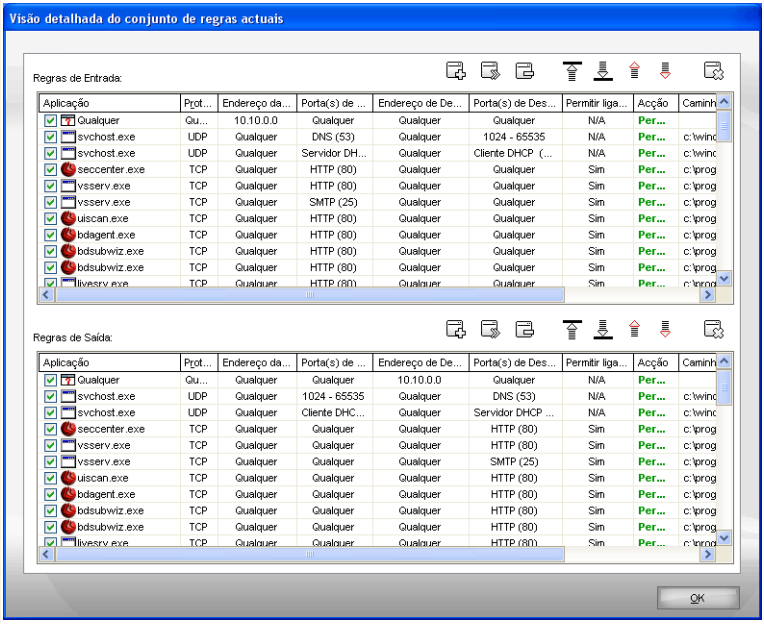
Para apagar uma regra, seleccione-a e clique no botão **Apagar Regra**.

Para modificar uma regra, seleccione-a e clique no botão **Editar Regra** ou faça duplo-clique sobre ela.

Nota
Um menu contextual encontra-se disponível e contém as seguintes opções: **Adicionar regra**, **Apagar regra** e **Editar regra**.

9.3.4. Modificar Perfis

Pode modificar um perfil ao clicar em **Editar perfil**. Irá abrir-se a seguinte janela:



Visão Detalhada

As regras estão divididas em 2 secções: regras de saída e regras de entrada. Pode ver a aplicação e os parâmetros da regra de cada uma delas (endereço origem, endereço destino, porta de origem, porta de destino, acção, etc.)

Para apagar uma regra, seleccione-a e clique no botão **Apagar regra**. Para apagar todas as regras clique no botão **Limpar lista**. Para modificar uma regra seleccione-a e clique no botão **Editar regra** ou faça duplo-clique nela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

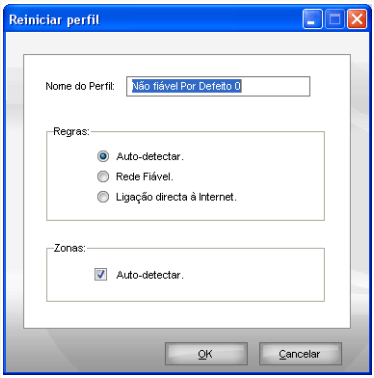
Pode aumentar ou diminuir a prioridade de uma regra. Clique no botão **Subir na Lista** para aumentar um nível a prioridade da regra seleccionada, ou clique no botão **Descer na Lista** para diminuir um nível a prioridade da regra seleccionada. Para atribuir a máxima prioridade a uma regra, clique no botão **Subir Topo**. Para atribuir a uma regra a miníma prioridade, clique no botão **Descer Fundo** .

Nota
Um menu contextual encontra-se disponível e contém as seguintes opções: **Adicionar regra**, **Editar regra**, **Apagar regra**, **Subir**, **Descer**, **Subir Topo**, **Descer Fundo** e **Limpar lista**.

Clique em **OK** para fechar a janela.

9.3.5. Reiniciar Perfis

Os utilizadores avançados podem escolher reconfigurar o perfil da firewall de forma a optimizar a protecção firewall ou personalizá-la de acordo com as suas necessidades. Pode reiniciar um perfil de firewall ao clicar em **Reiniciar perfil**. A seguinte análise irá aparecer:



Reiniciar Perfil

Pode configurar o seguinte:

- **Nome Perfil** - insira um novo nome no campo editável.
- **Regras** - especifique que tipo de regras devem ser criadas para as aplicações do sistema.

  Estão disponíveis as seguintes opções:

Opção	Descrição
Auto-detectar	Deixa que o BitDefender detecte a configuração de rede e cria um conjunto apropriado de regras elementares.
Rede Fiável	Cria um conjunto apropriado de regras elementares para uma rede fiável.
ligação Directa à Internet	Cria um conjunto apropriado de regras elementares para uma ligação directa à Internet.

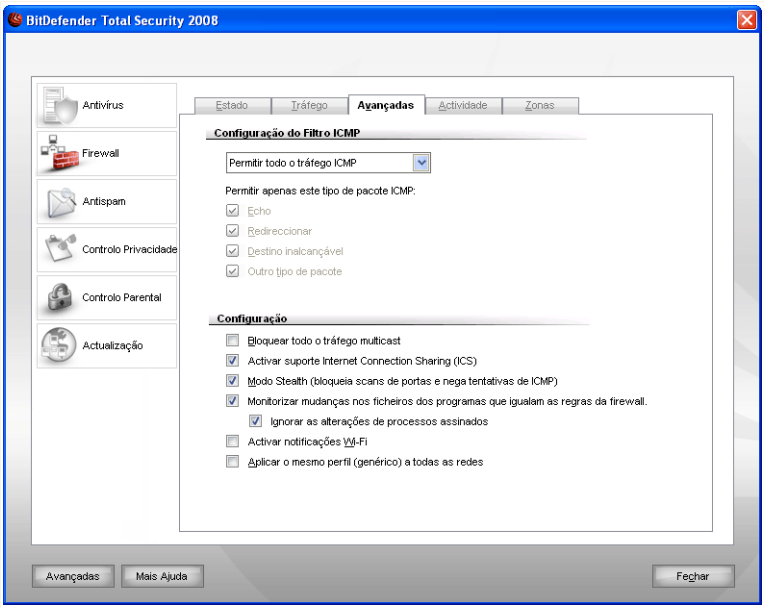
- **Zonas** - seleccione **Auto-detectar** para deixar que o BitDefender crie as zonas apropriadas para as redes detectadas.

Clique em **OK** para fechar a janela e reiniciar o perfil.

Importante
Todas as regras que adicionou nesta secção serão perdidas se decidir reconfigurar o perfil de firewall.

9.4. Configuração Avançada

Para configurar as definições avançadas da firewall BitDefender, clique em **Firewall>Avançada** na consola de configuração. A seguinte análise irá aparecer:



Configuração Avançada

Nesta secção pode definir a configuração avançada da firewall BitDefender. A configuração avançada permite-lhe especificar as regras de filtragem para o tráfego ICMP (Configuração Filtro ICMP) e bloquear o tráfego multicast, partilhar a sua ligação à Internet ou tornar o seu computador invisível ao software malicioso e aos hackers (Configuração).

9.4.1. Configurações Filtro ICMP

A partir do menu, pode seleccionar uma das seguintes políticas para filtrar o tráfego ICMP:

- **Permitir todo tráfego ICMP** - Permite todo o tráfego ICMP.
- **Bloquear todo tráfego ICMP** - Bloqueia todo o tráfego ICMP.
- **Filtragem ICMP personalizada** - personaliza a forma como o tráfego ICMP é filtrado. Poderá escolher que tipo de pacotes ICMP a permitir.

  Estão disponíveis as seguintes opções:

Opção	Descrição
Echo	Esta opção activa as mensagens do Echo Reply e do Echo Request. O Echo Request é uma mensagem do ICMP que envia um pacote de dados para o host e espera que esses dados sejam enviados de volta em Echo Reply. O host deve responder a todos os Echo Requests com um Echo Reply contendo exactamente os mesmos dados recebidos na mensagem de pedido. O Echo Reply é uma mensagem ICMP gerada em resposta a uma mensagem ICMP Echo Request, e é mandatária para todos os hosts e routers.
Redireccionar	Esta é uma mensagem ICMP que informa o host para redireccionar a sua informação de routing (para enviar os pacotes por um caminho alternativo). Se o host tentar enviar dados através de um router (R1) e depois outro router (R2) alcançar o host, e está disponível um caminho directo do host para o R2, o redireccionar informará o host de tal caminho. O router ainda enviará o datagram original para o destino pretendido. No entanto se o datagram contiver informação de routing, esta mensagem não será enviada mesmo que um melhor caminho esteja disponível.
Destino inalcançável	Isto é uma mensagem ICMP que é gerada pelo router para informar o cliente que o host de destino se encontra inalcançável, a não ser que o datagram tenha um endereço multicast. As razões para esta mensagem podem significar que a ligação física para o host não existe (a distância é infinita), o protocolo ou porta indicados não estão activos, ou os dados devem de estar fragmentados mas a flag 'não fragmentar' está activa.
Outro tipo de pacote	Com esta opção activa qualquer outro pacote para além de **Echo**, **Destino inalcançável** ou **Redireccionar** passará.

9.4.2. Configuração Avançada da Firewall

As seguintes configurações avançadas da firewall estão disponíveis:

- **Bloquear todo o tráfego multicast** - deixa cair qualquer pacote multicast recebido.

  O tráfego multicast é o tipo de tráfego que abrange um grupo especial na rede. Os pacotes são enviados para um endereço especial de onde o cliente multicast pode recebê-lo se ele concordar com isso.

  Por exemplo, um membro de uma rede que possui um sintonizador de TV pode transmitir (enviar para cada membro da rede) ou multicast (enviar para um endereço especial) o fluxo de vídeo. Os computadores que ouvem o endereço multicast podem aceitar ou rejeitar o pacote. Se aceitarem, o fluxo de vídeo pode ser visto pelos clientes multicast.

  Uma excessiva quantidade de multicast consome a largura de banda e os recursos. Com esta opção activada qualquer pacote multicast recebido será rejeitado. No entanto, não é recomendado seleccionar esta opção.
- **Activar Suporte de Internet Connection Sharing (ICS)** - activa o suporte para Internet Connection Sharing (ICS).

  Nota
  Esta opção não activa automaticamente o ICS no seu sistema, mas apenas permite este tipo de ligação em caso de a activar no seu sistema operativo.

  O Internet Connection Sharing (ICS) permite que elementos da sua rede de área local se liguem à Internet através do seu computador. Isto é útil quando benefecia de uma ligação à Internet especial/particular (ex:- ligação wireless) e a quer partilhar com outros membros da sua rede.

  Partilhar a sua ligação à Internet com membros da sua rede de área local leva a um elevado consumo de recursos e pode envolver algum risco. Também lhe retira algumas portas (aquelas abertas pelos membros que estão a usar a sua ligação à Internet).
- **Modo Stealth** - torna o seu computador invisível ao software malicioso e aos hackers.

  Uma maneira simples de descobrir se o seu computador está vulnerável é tentarem estabelecer ligação a portas e ver se há alguma resposta. Isto chama-se um scan de portas.

  Indivíduos ou programas com más intenções não necessitam de saber sequer que o seu computador existe, e menos ainda que providencia serviços à rede. A opção

do **Modo Stealth** faz com que a sua máquina deixe de responder a tentativas de procura de portas abertas ou da sua localização exacta.

- **Monitorizar mudanças em ficheiros de programas que igualam as regras da firewall** - Verifica cada tentativa de ligação à Internet das aplicações para ver se elas mudaram desde que a regra que controla o seu acesso foi criada. Se a aplicação foi alterada, um aviso de alerta surgirá para que permita ou bloquei o acesso da aplicação à Internet.

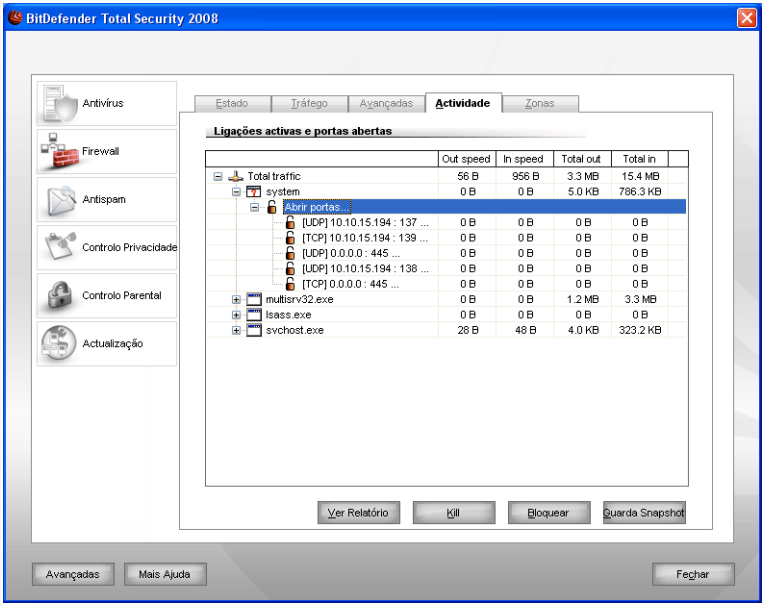
  Normalmente as aplicações são alteradas pelas actualizações. Mas, existe um risco que elas sejam alteradas por aplicações malware, com o propósito de infectar o seu computador e outros computadores na rede.

  Nota
  Recomendamos que mantenha esta opção seleccionada e permita acesso apenas àquelas aplicações que espera que tenham mudado após a regra que controla o seu acesso ter sido criada.

  Aplicações assinadas são suposta serem fiáveis e de um alto nível de segurança. Pode escolher **Ignorar mudanças em processos assinados** de forma a permitir que aplicações assinadas que se alteraram se liguem à Internet sem ser alertado acerca deste evento.
- **Activar notificações Wi-Fi** - activa as notificações Wi-Fi.
- **Aplica o mesmo (genérico) perfil a todas as novas redes** - cria um perfil de firewall por defeito (genérico, denominado `Rede Genérica`, e aplica-o sempre que uma nova configuração de rede é detectada. Se retroceder para uma antiga configuração de rede para a qul um perfil de firewall existe, o respectivo perfil de firewall é carregado em vez do perfil genérico.

9.5. Controlo de Ligação

Para monitorizar a rede actual / actividade Internet (em TCP e UDP) por aplicação e abrir o log da Firewall BitDefender, clique em **Firewall>Actividade** na consola de configuração. A seguinte análise irá aparecer:



Controlo de Ligação

Pode ver todo o tráfego por aplicação. Para cada aplicação, pode ver as ligações e as portas abertas, como também as estatísticas com respeito à velocidade de tráfego de saída & entrada e o montante total de dados enviados / recebidos.

A janela apresenta em tempo-real a actividade da actual rede / Internet. À medida que as ligações e portas são fechadas, pode ver que as estatísticas correspondentes são diminuidas e que, eventualmente, desaparecerão. A mesma coisa acontece a todas as estatísticas correspondentes a uma aplicação que gera tráfego ou que tem portas abertas que você fecha.

Clique em **Bloquear** para criar regras que restringem o tráfego da aplicação, porta ou ligação seleccionada. Será solicitado a confirmar a sua escolha. As regras podem ser acedidas na secção Tráfego para uma maior afinação.

Nota
Para bloquear uma aplicação, porta ou ligação, pode também fazer clique botão-direito do rato e seleccionar **Bloquear**.

Clique em **Kill** para terminar todas as instâncias de um determinado processo. Ser-lhe-á solicitado que confirme a sua escolha.

Nota
Para "kill" um processo, pode também clicar botão-direito do rato e seleccionar **Kill**.

Clique em **Guarda Snapshot** para exportar a lista para um ficheiro `.txt`.

Para obter uma lista mais completa de eventos com respeito ao uso do módulo da Firewall (iniciar/parar a firewall, bloquear tráfego, activar Modo Stealth, modificar configurações, aplicar um perfil) ou gerado pelas actividades detectadas por ela (scan de portas, bloqueio de tentativas de ligação ou de tráfego de acordo com as regras) consulte o ficheiro de relatório da Firewall do BitDefender que pode ser visualizado clicando em **Mostrar Relatório**. O ficheiro está localizado na pasta Ficheiros Comuns do actual utilizador do Windows, no caminho: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

9.6. Zonas de Rede

Uma zona é um endereço IP ou um leque de endereços IP para os quais uma regra especial é criada dentro de um perfil. A regra pode permitir aos membros da rede um acesso ilimitado ao seu computador (zonas fiáveis) ou, pelo contrário, isolar completamente o seu computador dos outros computadores da rede (zona não-fiável).

Por defeito, o BitDefender detecta automaticamente a rede a que está ligado e adiciona uma zona dependendo da configuração de rede.

Nota
Se está ligado a várias redes, dependendo da configuração, uma ou mais zonas podem ser adicionadas.

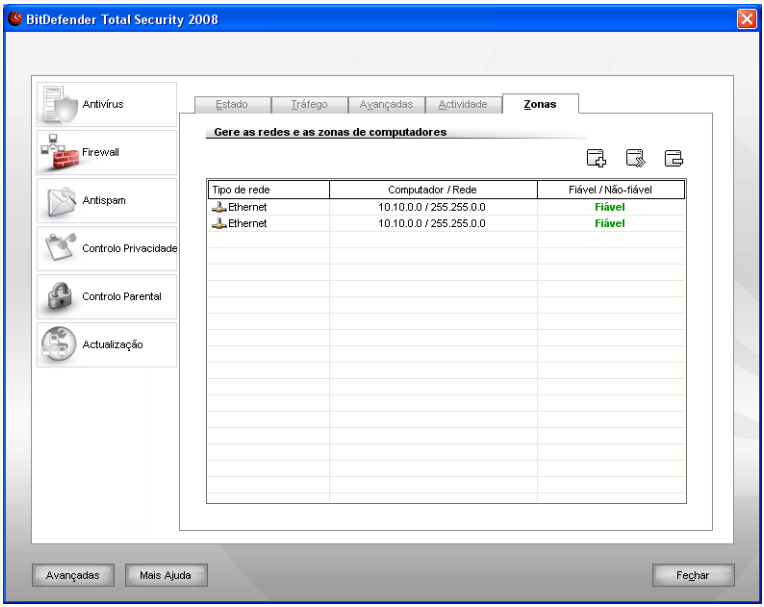
Zonas fiáveis são adicionadas por defeito para as seguintes configurações de rede:

- **IP fixo sem gateway** - O computador faz parte de uma rede de área local (LAN) e não se liga à Internet.
- **IP Privado com Controlador de Domínio detectado** - O computador faz parte de uma rede da àrea local (LAN) e está ligado a um domínio.

Zonas não-fiáveis são adicionadas por defeito para as seguintes configurações de rede:

- **Wireless Aberta (não segura)** - O computador faz parte de uma rede da área local wireless (WLAN).

Para gerira as zonas de rede, clique em **Firewall>Zonas** na consola de configuração. A seguinte análise irá aparecer:



Zonas de Rede

Pode ver as zonas de rede correspondentes ao perfial actual listado na tabela. Para cada zona pode ver o tipo de rede ((Ethernet, wireless, PPP e por ái fora), o computador ou a rede associado a essa zona e se a zona é fiável ou não-fiável.

Para modificar uma zona, seleccione-a e clique no botão **Editar Zona** ou faça duplo clique sobre ela.

Nota

Por defeito, o BitDefender adiciona a redes wireless abertas como zona não-fiáveis. Se está ligado a uma rede wireless aberta ad-hoc com computadores fiáveis (em casa ou com um conjunto de amigos), poderá querer editar a zona associada. De forma a

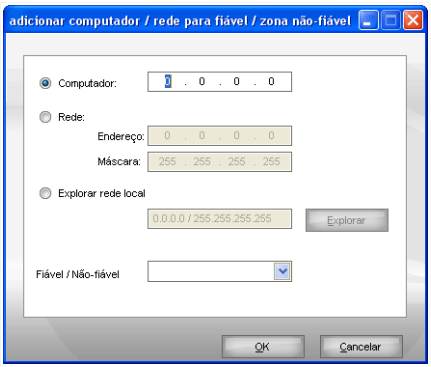
ser capaz de partilhar recursos com outros membros da rede, pode definir a rede como uma zona fiável.

Para apagar uma zona, seleccione-a e clique no botão **Apagar Zona** .

9.6.1. Adicionar Zonas

Pode adicionar zonas manualmente. Isto permite-lhe, por exemplo, partilhar ficheiros apenas com os seus amigos dentro de uma rede wireless aberta (ao adicionar os seus computadores como zonas fiáveis), ou a bloquear um computador de uma rede fiável (ao adicioná-lo como uma zona não-fiável).

Para adicionar uma zona, clique no botão **Adicionar Zona** . A seguinte análise irá aparecer:



Adicionar Zona

Para adicionar uma zona, siga estes passos:

1. Especificar um computador de uma rede local ou uma rede local inteira que queira adicionar como uma zona. Pode usar um dos seguintes métodos:
   - Para adicionar um determinado computador, seleccione **Computador** e forneça o seu endereço IP.
   - Para adicionar uma rede, seleccione **Rede** e forneça o seu endereço IP e máscara.
   - Explorar as redes locais e descobrir e adicionar um computador ou uma rede.

Para explorar as redes locais, seleccione **Explorar rede local** e depois clique em **Explorar**. Uma nova janela aparecerá onde pode ver todas as redes a que está ligado como também todos os membros da cada rede.

Seleccione a partir da lista o computador ou rede que deseja que seja adicionado como zona e clique em **OK**

2. Seleccione a partir do menu que tipo de zona deseja criar (fiável ou não-fiável).
3. Clique em **OK** para adicionar a zona.

10. Antispam

O BitDefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes de o mesmo chegar à caixa de correio A receber do utilizador.

A secção do **Antispam** deste guia do utilizador contém os seguintes tópicos:

- Compreender o Antispam
- Estado do Antispam
- Configurações de Antispam
- Integração com Clientes de Mail

10.1. Compreender o Antispam

O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

10.1.1. Filtros Antispam

O Motor Antispam do BitDefender Antispam incorpora sete filtros distintos, os quais asseguram que a sua Caixa de Entrada de correio se mantenha livre de SPAM: Lista Branca, Lista Negra, Filtro caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano.

Nota
Pode activar/desactivar cada um destes filtros na secção da Configuração no módulo de **Antispam**.

Lista Branca / Lista Negra

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Nota
A **Lista Branca / Lista Negra** também são conhecidas como **Lista de Amigos / Lista de Spammers**.

Pode gerir a **Lista de Amigos / Lista de Spammers** através da Consola de Configuração ou através da Barra de ferramentas do Antispam integrada em alguns dos clientes de mail mais utilizados.

Nota
Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Filtro de caracteres

A maioria das mensagens de spam estão escritas em caracteres Cirílicos ou Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

Filtro de Imagem

Uma vez que evitar o filtro heurístico se tornou um desafio e tanto, hoje em dia as pastas de entrada dos e-mails estão cada vez mais cheias de mensagens contendo apenas uma imagem com conteúdo não-solicitado. Para fazer face a este problema crescente, BitDefender introduziu o **Filtro de Imagem** que compara a assinatura do e-mail com aquelas da base de dados do BitDefender. Em caso de igualdade o e-mail será etiquetado como SPAM.

Filtro URL

A maioria das mensagens de Spam contém links para vários locais da web. Estes locais por sua vez contém mais publicidade e a possibilidade de comprar coisas, e por vezes, são usados para phishing.

O BitDefender mantém uma base de dados de tais links. O filtro URL verificas cada link URL numa mensagem e compara-o com a sua base de dados. Se existir uma correspondência, a mensagem é marcada como SPAM.

Filtro NeuNet (Heurístico)

O **Filtro NeuNet (Heurístico)** executa uma série de testes nos componentes da mensagem (por ex., não só o cabeçalho mas também todo o corpo da mensagem, seja em formato HTML ou em texto), procurando palavras, frases, links ou outras

características de SPAM. Baseado nos resultados da análise, adiciona uma marca de SPAM à mensagem.

O filtro também detecta mensagens marcadas como `SEXUALMENTE EXPLÍCITO:` no assunto e marca-as como SPAM.

Nota
Desde 19 de Maio de 2004, o Spam com conteúdo de caracter sexual, tem de incluir o aviso SEXUALMENTE EXPLÍCITO: no assunto ou está sujeito a multa por violação da lei.

Filtro Bayesiano

O módulo do **Filtro Bayesiano** classifica as mensagens de acordo com informações estatísticas, que indicam a frequência com que determinadas palavras aparecem nas mensagens classificadas como SPAM, quando comparadas com aquelas que não são consideradas SPAM (por si ou pelo filtro heurístico).

Isto significa, por exemplo, se uma certa palavro de quatro letras aparece com mais frequência no SPAM, é natural assumir que existe uma maior probabilidade da próxima mensagem que a inclua, seja SPAM. São levadas em conta, todas as palavras relevantes dentro de uma mensagem. Após sintetizar a informação estatística, é computada a probabilidade da mensagem ser SPAM.

Este módulo apresenta outra característica interessante: é treinável. Adapta-se rapidamente ao tipo de mensagens recebidas pelo utilizador, e armazena informação acerca de todas elas. Para funcionar com eficácia, o filtro tem de ser treinado, o que significa, apresentar-lhe amostras de Spam e de mensagens legítimas, tal como um cão de caça é treinado a caçar uma certa presa. Ás vezes o filtro também tem de ser corrigido – ajustado quando toma uma decisão errada.

Importante
Pode corrigir o módulo Bayesiano ao usar os botões **É Spam** e **Não é Spam** da Barra de tarefas Antispam.

Nota
Cada vez que executa uma actualização:

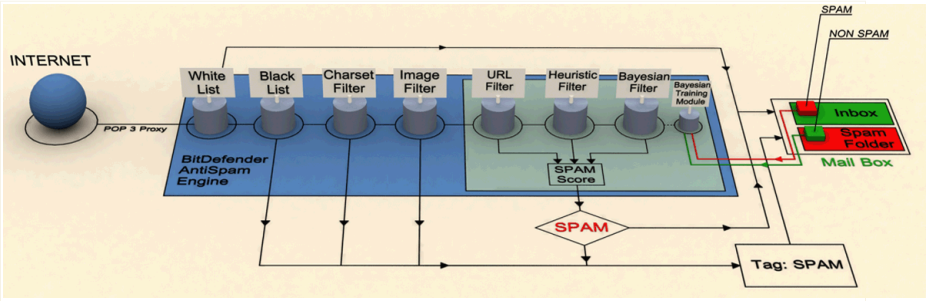
- novas assinaturas de imagens serão adicionadas ao **Filtro de Imagem**.
- novos links serão adicionados ao **Filtro de URL**.
- novas regras serão adicionadas ao **filtro NeuNet (Heurístico)**.

Isto ajuda a aumentar a eficácia do motor Antispam.

Para o proteger contra os spammers, BitDefender pode levar a cabo actualizações automáticas. Mantenha a opção **Actualização Automática** activa.

10.1.2. Operação Antispam

O esquema abaixo mostra como o BitDefender funciona.



Operação Antispam

Os filtros antispam do esquema acima (Lista Branca, Lista Negra, Filtro de caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano) são usados em conjunto pelo módulo Antispam do BitDefender, para determinar se uma determinada partícula de e-mail deve chegar à sua **Caixa de Entrada** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Branca/Lista Negra. Se o endereço do remetente se encontrar na Lista Branca, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista Negra irá apoderar-se do seu e-mail para verificar se o endereço do remetente se encontra na lista. O e-mail será marcado como SPAM e movido para a pasta de **Spam** (localizado no Microsoft Outlook) se houver uma correspondência.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado como SPAM e movido para a pasta de **Spam**.

Se o e-mail não estiver escrito em caracteres Cirílicos ou Asiáticos, irá passar pelo Filtro de Imagem. O **Filtro de Imagem** detecta todas as mensagens de e-mail que contêm imagens anexadas com conteúdo de spam.

O Filtro URL irá procurar ligações e compará-las às ligações da base de dados do BitDefender. Em caso de corresponder, irá adiconar ao e-mail uma marca de SPAM.

O Filtro NeuNet (Heurístico) irá apoderar-se do e-mail e irá executar uma série de testes aos componentes da mensagem, procurando palavras, frases, links e outras características de SPAM. E o e-mail, dependendo do resultado será ou não marcado como SPAM.

Nota

Se o e-mail estiver marcado como SEXUALMENTE EXPLICITO na linha do assunto, o BitDefender irá considerá-lo como SPAM.

O módulo do Filtro Bayesiano irá seguidamente analisar a mensagem, de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como SPAM, comparadas com aquelas que não são SPAM (por si ou pelo filtro heurístico). Irá ser adicionada à mensagem uma marca de Spam.

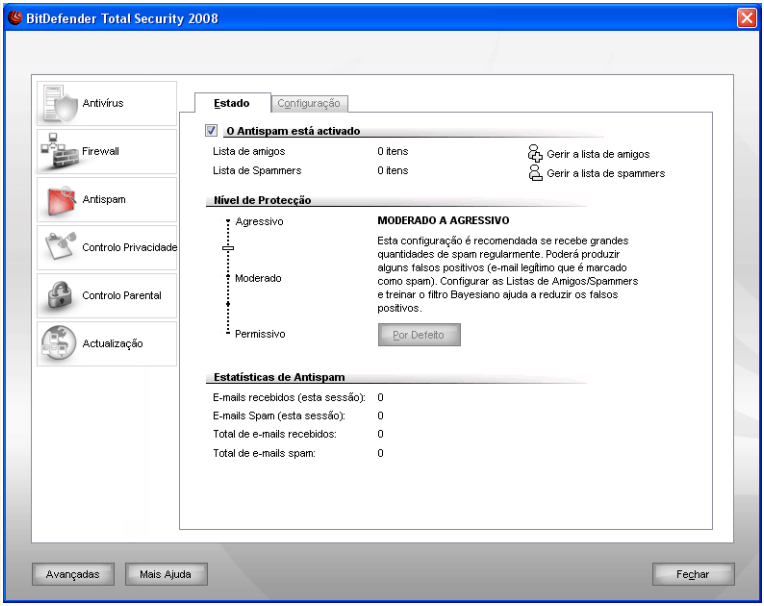
Se a pontuação total (pontuação URL + pontuação heurística + pontuação Bayesiana) excederam a pontuação de SPAM para uma mensagem (definida pelo utilizador na secção Estado como nível de tolerância), a mensagem é considerada SPAM.

Importante

Se está a utilizar outro outro cliente de e-mail que não seja o Microsoft Outlook ou Microsoft Outlook Express deve criar uma regra para mover as mensagens de e-mail maracadas como SPAM pelo BitDefender para uma pasta de quarentena que use regularmente. O BitDefender anexa o prefixo `[SPAM]` ao assunto das mensagens consideradas como tal.

10.2. Estado do Antispam

Para configurar a protecção Antispam, clique em **Antispam>Estado** na consola de configuração. A seguinte análise irá aparecer:



Estado do Antispam

Nesta secção pode configurar o módulo de **Antispam** e pode visualizar informação acerca da sua actividade.

Importante
Para prevenir a entrada de Spam na sua **Caixa de Entrada**, mantenha activo o **Filtro Antispam**.

Na secção das **Estatísticas** pode visualizar as estatísticas que dizem respeito ao módulo de Antispam. Os resultados são apresentados por sessão (desde que iniciar o seu computador) ou pode ver um sumário da actividade de Antispam desde a instalação do Filtro de Antispam.

Para configurar o módulo de **Antispam** é necessário proceder da seguinte maneira:

10.2.1. Passo 1/2 - Definir o Nível de Tolerância

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 5 níveis de tolerância:

Nível de Tolerância	Descrição
Tolerante	Oferece protecção às contas que recebem uma grande quantidade de e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).
Tolerante a Moderado	Oferece protecção às contas que recebem alguns e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).
Moderado	Oferece protecção às contas regulares. O filtro bloqueará a maioria do spam, enquanto evita falsos positivos.
Moderado a Agressivo	Oferece protecção às contas que recebem uma grande quantidade de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam). Configura as **Listas de Amigos/Spammers** e treina o **Motor de Aprendizagem (Bayesiano)** de forma a reduzir o número de falsos positivos.
Agressivo	Oferece protecção a contas que recebem um volume muito elevado de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam).

Nível de Tolerância	Descrição
	Adicione os seus contactos à **Lista de Amigos** de forma a reduzir o número de falsos positivos.

Para definir o nível de protecção por defeito (**Moderado a Agressivo**) clique em **Nível por Defeito**.

10.2.2. Passo 2/2 - Preencher a Lista de Endereços

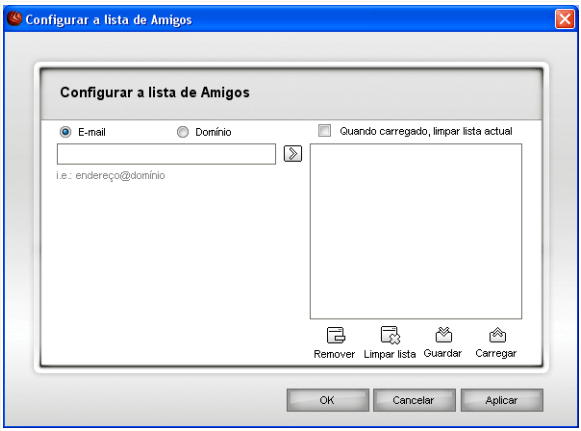
As listas de endereços contêm informação acerca dos endereços de e-mail que lhe enviam mensagens de e-mail legítimas ou spam.

Lista de Amigos

A **Lista de amigos** é uma lista de todos os endereços de e-mail, dos quais deseja receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

Nota
Qualquer e-mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada.

Para gerir a **Lista de amigos** clique em (correspondente à **Lista de amigos**) ou clique no botão **Amigos** na Barra de tarefas Antispam.



Lista de Amigos

Aqui pode adicionar ou remover entradas da **Lista de amigos**.

Se quiser adicionar um endereço de e-mail seleccione a opção **E-mail** introduza-o e clique no botão ⊠. O endereço irá aparecer na **Lista de amigos**.

Importante
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique no botão ⊠. O domínio irá aparecer na **Lista de amigos**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de amigos** para/de um local desejado. O ficheiro irá ter a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota
Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

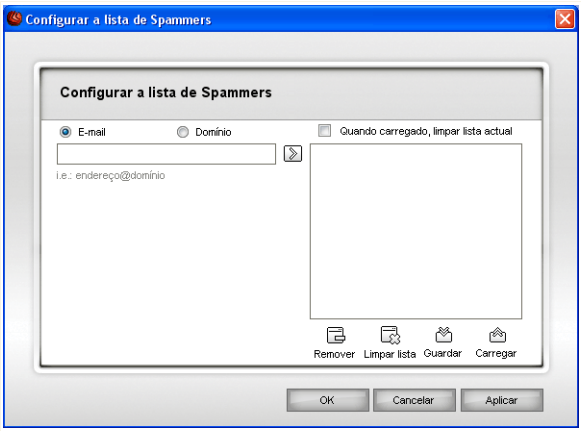
Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de amigos**.

Lista de Spammers

A **Lista de Spammers** é uma lista de todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo.

Nota
Todo o e-mail proveniente de um endereço presente na **Lista de Spammers**, será marcado automaticamente como SPAM.

Para gerir a **Lista de spammers** clique em (correspondente à **Lista de spammers**) ou clique no botão **Spammers** na Barra de tarefas Antispam.



Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de Spammers**.

Se quiser adicionar um endereço de email seleccione a opção **E-mail**, insira o endereço e clique no botão . O endereço irá aparecer na **Lista de spammers** .

Importante
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção**Domínio**, insira-o e clique no botão . O domínio irá aparecer na **Lista de spammers**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os e-mails provenientes de dominio.com serão marcados como SPAM;
- *dominio* - todos os e-mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como SPAM;
- *com - todos os e-mails tendo o sufixo de domínio com serão marcados como SPAM.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de spammers** para/de o local desejado. O ficheiro terá a extensão `.bwl`.

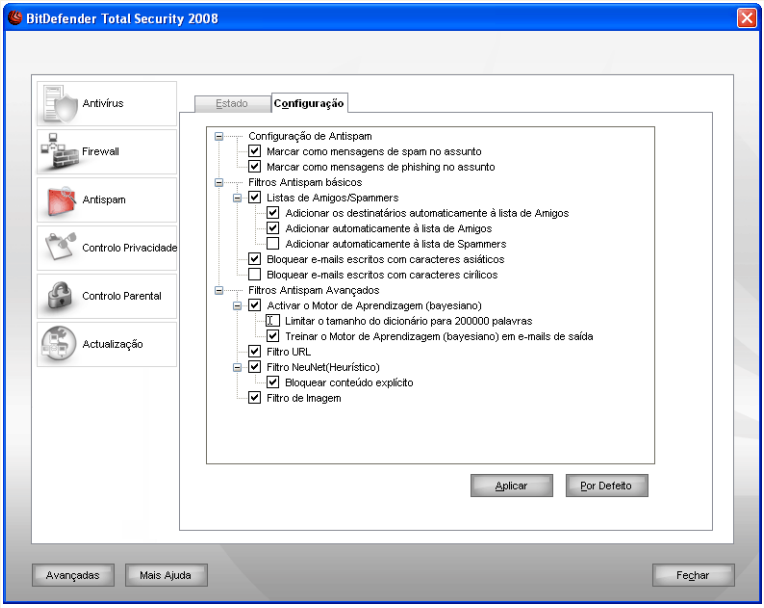
Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de Spammers**.

Importante
Se deseja reinstalar o BitDefender será uma boa ideia guardar as listas de **Amigos** / **Spammers**, antes do processo de reinstalação, e após o processo de reinstalação ter terminado pode carregá-las.

10.3. Configurações de Antispam

Para configurar as definições de antispam, clique em **Antispam>Definições** na consola de configuração. A seguinte análise irá aparecer:



Configurações de Antispam

Aqui pode activar/desactivar cada um dos filtros Antispam e pode especificar outras definições com respeito ao módulo Antispam.

Encontram-se disponíveis três categorias de opções (**Configuração de Antispam**, **Filtros básicos de Antispam** e **Filtros avançados de Antispam**) organizadas num menu expansível, semelhante aos do Windows.

Nota
Clique na caixa marcada com o sinal "+" para abrir a categoria ou clique na que está marcada com o sinal "-" para fechar a categoria.

10.3.1. Configurações de Antispam

- **Marcar como mensagem de spam no assunto** - todas as mensagens de e-mail consideradas spam serão marcadas como SPAM no assunto.
- **Marcar mensagens phishing no assunto** - todas as mensagens de e-mail consideradas mensagens de phishing serão marcadas como SPAM na linha do assunto.

10.3.2. Filtros Antispam Básicos

- **Listas de amigos / spammers** - activa/desactiva as Listas de amigos / spammers;
  - **Adicionar automaticamente à lista de Amigos** - para adicionar os destinatários de e-mails enviados à Lista de Amigos.
  - **Adicionar automaticamente à Lista de amigos** - da próxima vez que clicar no botão **Não-Spam** na Barra de tarefas Antispamo remetente será automaticamente adicionado à **Lista de amigos**.
  - **Adicionar automaticamente à Lista de Spammers** - da próxima vez que clicar no botão **É Spam** na Barra de tarefas Antispam o remetente será automaticamente adicionado à **Lista de Spammers**.

  Nota
  Os botões **Não-Spam** e **É Spam** são usados para treinar o filtro Bayesiano.

- **Bloquear Asiático** - bloqueia mensagens escritas com Caracteres asiáticos.
- **Bloquear Cirílico** - bloqueia mensagens escritas com Caracteres cirílicos.

10.3.3. Filtros Antispam Avançados

- **Activar Motor de Aprendizagem (bayesiano)** - activa/desactiva o Motor de Aprendizagem (bayesiano);
  - **Limitar o tamanho do dicionário para 200000 palavras** - com esta opção pode estabelecer o tamanho do dicionário Bayesian – quanto menor mais rápido, maior é mais eficaz.

Nota
O tamanho recomendado é de: 200.000 palavras.

  - **Treinar Motor de Aprendizagem (bayesiano) nos e-mails de saída** - treina o Motor de Aprendizagem (bayesiano) nos e-mails de saída.
- **Filtro URL** - activa/desactiva o Filtro URL;
- **Filtro NeuNet (Heurístico)** - activa/desactiva o Filtro NeuNet (Heurístico);
  - **Bloquear conteúdo explícito** - activa/desactiva a detecção de mensagens com o aviso de conteúdo SEXUALMENTE EXPLÍCITO na linha do assunto.
- **Filtro de Imagem** - activa/desactiva o Filtro de Imagem.

Nota
Para activar/desactivar uma opção seleccione/limpe a caixa de selecção correspondente a ela.

Clique em **Aplicar** para guardar as alterações, ou clique em **Nível por Defeito** para carregar as definições por defeito.

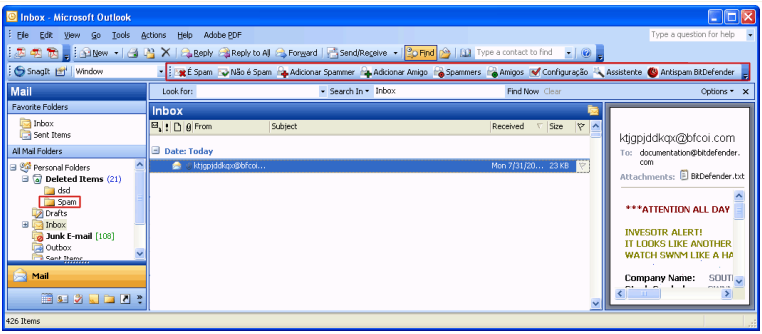
10.4. Integração com Clientes de Mail

BitDefender integra-se directamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes clientes de mail:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

10.4.1. Barra de Ferramentas do Antispam

No lado superior do seu cliente de mail pode ver a barra de ferramentas do Antispam.



Barra de Ferramentas do Antispam

Importante

A diferença entre o BitDefender Antispam para o Microsoft Outlook e o do Outlook Express/ Windows Mail, é que as mensagens SPAM são movidas para a pasta de **Spam** para o Microsoft Outlook e no Outlook Express elas são movidas para a pasta **Itens Eliminados**. Em ambos os casos as mensagens são marcadas como SPAM, na linha do assunto.

A pasta de **Spam** é criada automaticamente pelo BitDefender no Microsoft Outlook e é listada ao mesmo nível com os itens da **Lista de Pastas**(Calendário, Contactos, etc).

Cada botão da barra de tarefas BitDefender é explicado abaixo:

- **É Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado é spam. O e-mail será marcado como SPAM e será movido para a pasta de **Spam**.

  As futuras mensagens de e-mail que se enquadrem no mesmo padrão serão marcadas como SPAM.

  Nota

  Pode seleccionar uma mensagem de e-mail ou tantas quantas desejar.

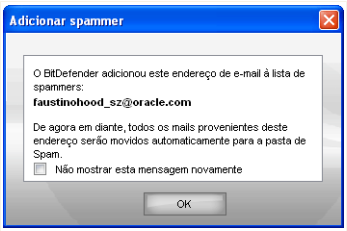
- **Não é Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado não é spam, e que o BitDefender não o deve marcar como tal. O e-mail será movido da pasta de **Spam** para o directório da **Caixa de Entrada**.

As futuras mensagens de e-mail que se enquadrem no mesmo padrão não serão marcadas como SPAM.

Nota
Pode seleccionar uma mensagem de e-mail ou tantas quantas desejar.

Importante
O botão **Não é Spam** fica activo quando seleccionar uma mensagem marcada como SPAM pelo BitDefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

- **Adicionar spammer** - adiciona o remetente da mensagen seleccionada à **Lista de Spammers**.


Adicionar spammer
O BitDefender adicionou este endereço de e-mail à lista de spammers:
faustinohood_sz@oracle.com
De agora em diante, todos os mails provenientes deste endereço serão movidos automaticamente para a pasta de Spam.
Não mostrar esta mensagem novamente
OK

Adicionar Spammer

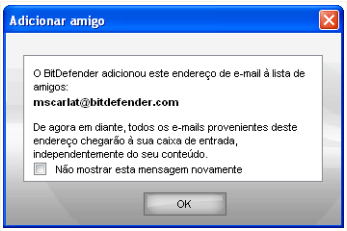
Seleccione **Não mostrar esta mensagem novamente** se não quer ser consultado para confirmação, quando adiciona à lista um endereço de um spammer.

Clique em **OK** para fechar a janela.

As futuras mensagens de e-mail provenientes desses endereços serão marcadas como SPAM.

Nota
Pode seleccionar um remetente ou tantos quantos desejar.

- **Adicionar Amigo** - adiciona o remetente das mensagens seleccionadas à sua **Lista de Amigos**.


Adicionar amigo
O BitDefender adicionou este endereço de e-mail à lista de amigos:
mscarlat@bitdefender.com
De agora em diante, todos os e-mails provenientes deste endereço chegarão à sua caixa de entrada, independentemente do seu conteúdo.
Não mostrar esta mensagem novamente
OK

Adicionar Amigo

Seleccione **Não mostrar esta mensagem novamente** se não quer ser consultado para confirmação, quando adiciona à lista um endereço amigo.

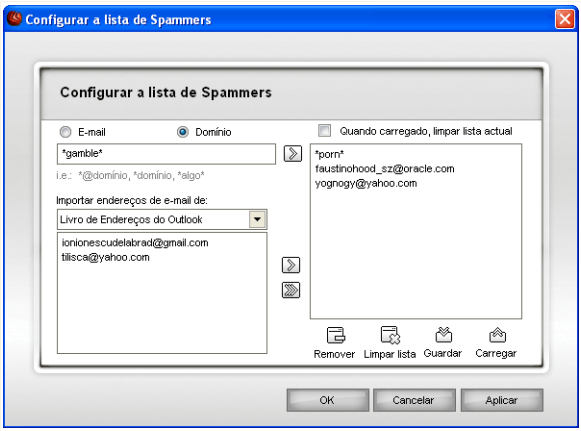
Clique em **OK** para fechar a janela.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo dos mesmos.

Nota
Pode seleccionar um remetente ou tantos quantos desejar.

- **Spammers** - abre a **Lista de Spammers** que contém todos os endereços de e-mail dos quais não deseja receber mensagens de e-mail, independentemente do seu conteúdo.

Nota
Todo o e-mail proveniente de um endereço presente na **Lista de Spammers**, será marcado automaticamente como SPAM.



Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de Spammers**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, introduza-o e clique no botão . Os endereços irão aparecer na **Lista de Spammers**.

Importante
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de Spammers**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os e-mails provenientes de dominio.com serão marcados como SPAM;
- *dominio* - todos os e-mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como SPAM;
- *com - todos os e-mails tendo o sufixo de domínio com serão marcados como SPAM.

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail**

seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express/ Windows Mail** aparecerá uma nova janela de onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de spammers**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os que deseja e clique em para os adicionar à **Lista de Spammers**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

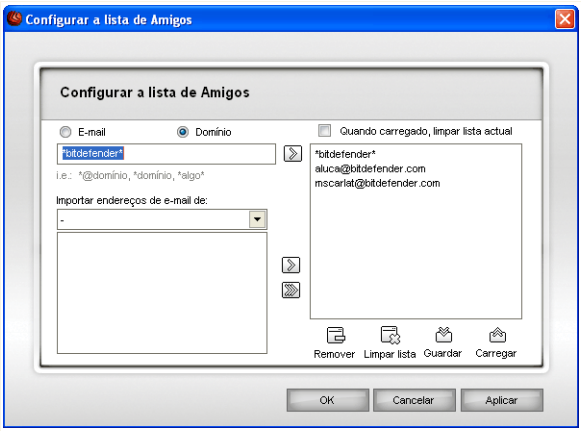
Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de spammers** para/de o local desejado. O ficheiro terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de Spammers**.

- **Amigos** - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo.

> ***Nota***
> Qualquer e-mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada.



Lista de Amigos

Aqui pode adicionar ou remover entradas da **Lista de amigos**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, insira-o e clique no botão . O endereço irá aparecer na **Lista de amigos**.

Importante
Sintaxe: nome@dominio.com.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de amigos**.

Importante
Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail**

seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express / Windows Mail** aparecerá uma nova janela onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de Amigos**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os desejados e clique em para os adicionar à **Lista de Amigos**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

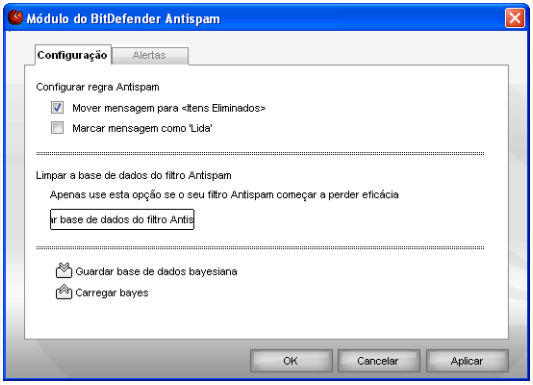
Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de amigos** para/de um local desejado. O ficheiro irá ter a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota
Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de amigos**.

- **Configuração** - abre a janela das **Configurações** onde pode definir algumas opções para o módulo **Antispam**.



Configuração

Estão disponíveis as seguintes opções:

- **Mover mensagens para Itens eliminados** - para mover as mensagens de spam para os **Itens eliminados** (apenas para o Microsoft Outlook Express / Windows Mail);
- **Marcar mensagem como 'Lida'** - para marcar todas as mensagens Spam como lidas, para que, quando chegarem novas mensagens spam não seja incomodado.

Se o seu filtro Antispam for muito impreciso, pode necessitar de limpar a base de dados do filtro e voltar a treinar o Filtro Bayesiano. Clique em **Limpar dados do filtro Antispam** se pretende fazer reset à base de dados do filtro Bayesiano.

Utilize os botões **Guardar bayes**/ **Carregar bayes** para guardar/carregar a lista da base de dados Bayesiana para um local desejado. O ficheiro terá uma extensão `.dat`.

Clique no botão **Alertas** se deseja aceder à secção onde poderá desactivar a aparição da janela de confirmação para os botões **Adicionar Spammer** e **Adicionar Amigo**.

Nota

Na janela de **Alertas** pode activar/desactivar a aparição do alerta **Por favor seleccione um e-email** . Este alerta surge quando selecciona um grupo em vez uma mensagem de e-mail.

- **Assistente** - abre o assistente que irá guiá-lo através do processo de treino do Filtro Bayesiano, para que a eficácia do BitDefender Antispam seja aumentada.

Também pode adicionar endereços do seu **Livro de Endereços** à sua **lista de Amigos** / **lista de Spammers**.

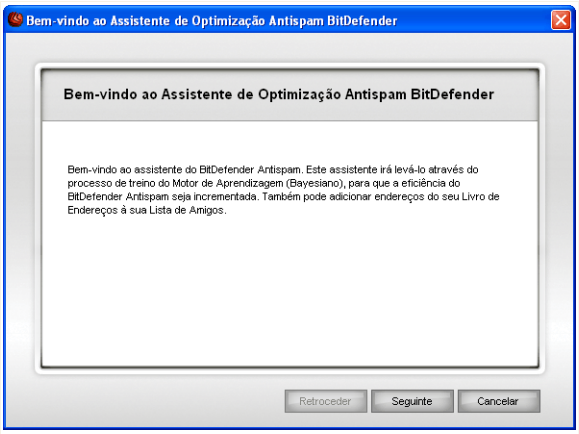
- **BitDefender Antispam** - abre a Consola de Administração.

10.4.2. Assistente de Configuração Antispam

Após ter instalado o seu BitDefender e na primeira vez que executar o seu cliente de Mail, um assistente irá aparecer para o ajudar a configurar a Lista de Amigos e a Lista de Spammers e a treinar o Filtro Bayesiano, para aumentar a eficiência dos filtros Antispam.

Nota
O assistente pode ser executado a qualquer altura que deseje clicando no botão **Assistente** na Barra de tarefas Antispam.

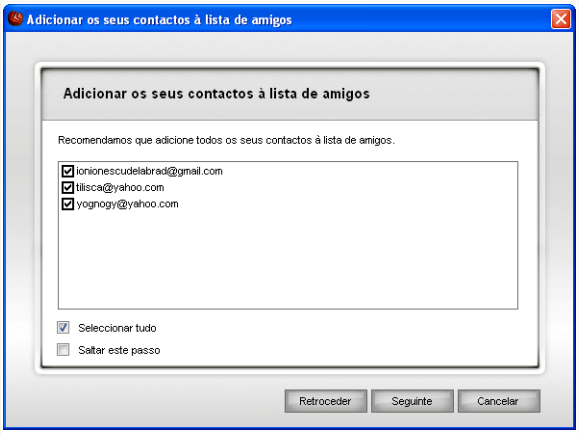
Passo 1/6 - Janela de Boas-vindas


Bem-vindo ao Assistente de Optimização Antispam BitDefender
Bem-vindo ao Assistente de Optimização Antispam BitDefender
Bem-vindo ao assistente do BitDefender Antispam. Este assistente irá levá-lo através do processo de treino do Motor de Aprendizagem (Bayesiano), para que a eficiência do BitDefender Antispam seja incrementada. Também pode adicionar endereços do seu Livro de Endereços à sua Lista de Amigos.
Retroceder
Seguinte
Cancelar

Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/6 - Preencher a Lista de Amigos



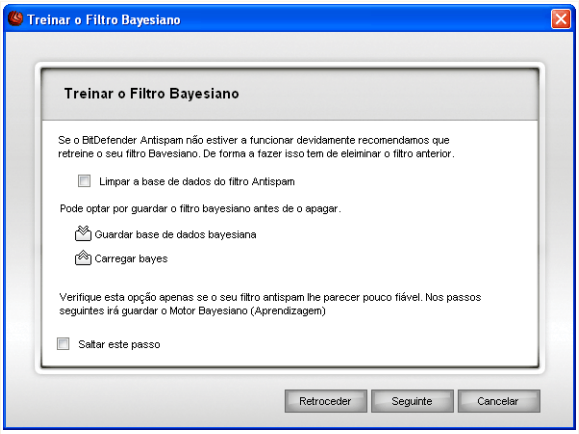
Preencher a Lista de Amigos

Aqui pode ver todos os endereços do seu **Livro de Endereços**. Por favor seleccione os que pretende adicionar à sua **Lista de Amigos** (recomendamos que seleccione todos). Irá receber todas as mensagens de e-mail desses endereços, independentemente do seu conteúdo.

Para adicionar todos os seus contactos à lista de Amigos, seleccione **Seleccionar todos**.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 3/6 - Apagar a Base de Dados Bayesiana


Treinar o Filtro Bayesiano
Treinar o Filtro Bayesiano
Se o BitDefender Antispam não estiver a funcionar devidamente recomendamos que retreine o seu filtro Bayesiano. De forma a fazer isso tem de eleiminar o filtro anterior.
Limpar a base de dados do filtro Antispam
Pode optar por guardar o filtro bayesiano antes de o apagar.
Guardar base de dados bayesiana
Carregar bayes
Verifique esta opção apenas se o seu filtro antispam lhe parecer pouco fiável. Nos passos seguintes irá guardar o Motor Bayesiano (Aprendizagem)
Saltar este passo
Retroceder
Seguinte
Cancelar

Apagar a Base de Dados Bayesiana

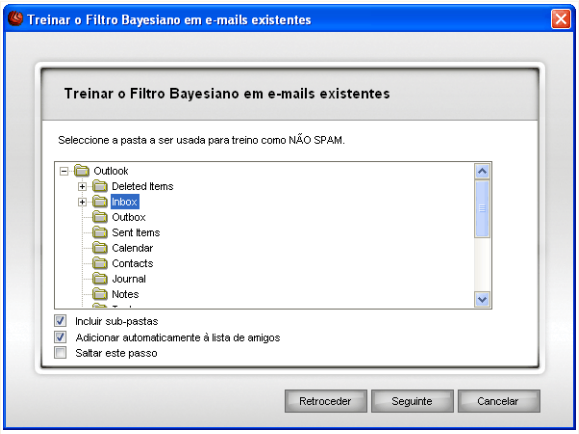
Poderá deparar-se com o facto do seu filtro de Antispam começado a perder eficácia. Isto pode estar relacionado com treino inapropriado (por ex. por erro, marcou um certo número de mensagens legítimas como spam, ou vice versa). Se o seu filtro for muito impreciso, poderá necessitar de limpar a base de dados e voltar a treinar o filtro seguindo os passos deste assistente.

Seleccione **Limpar dados do filtro Antispam** se pretende efectuar reset à base de dados do filtro Bayesiano.

Utilize os botões **Guardar bayes**/ **Carregar bayes** para guardar/carregar a lista da base de dados Bayesiana para um local desejado. O ficheiro terá uma extensão `.dat`.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 4/6 - Treinar o filtro Bayesiano com E-mails Legítimos



Treinar o filtro Bayesiano com E-mails Legítimos

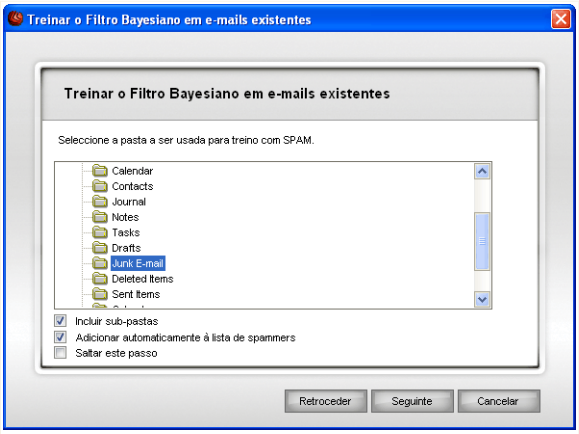
Por favor seleccione a pasta que contém mensagens de e-mail legítimas. Estas mensagens serão usadas para treinar o filtro Bayesiano.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adicionar automaticamente à lista de amigos** - para adicionar os remetentes à **Lista de Amigos**.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 5/6 - Treinar o filtro Bayesiano com Spam



Treinar o filtro Bayesiano com Spam

Por favor seleccione a pasta que contém mensagens de e-mail de spam. Estas mensagens serão usadas para treinar o filtro Bayesiano.

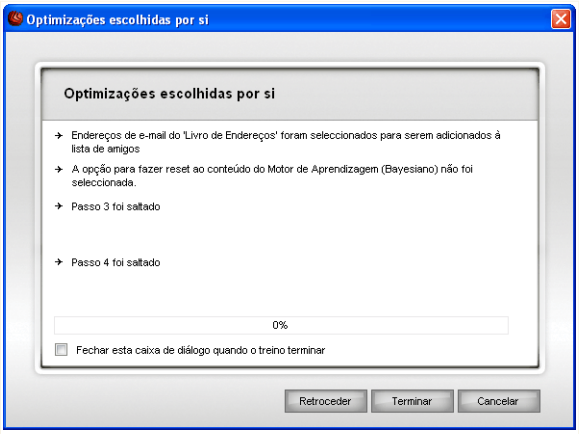
Importante
Por favor certifique-se que a pasta que escolher não contém, de modo algum, e-mails legítimos; de outro forma, o desempenho do Antispam será consideravelmente reduzido.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adiconar automaticamente à lista spammers** - para adicionar os remetentes à **Lista de Spammers**.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 6/6 - Resumo


Optimizações escolhidas por si
Optimizações escolhidas por si
Endereços de e-mail do 'Livro de Endereços' foram seleccionados para serem adicionados à lista de amigos
A opção para fazer reset ao conteúdo do Motor de Aprendizagem (Bayesiano) não foi seleccionada.
Passo 3 foi saltado
Passo 4 foi saltado
0%
Fechar esta caixa de diálogo quando o treino terminar
Retroceder
Terminar
Cancelar

Resumo

Nesta janela pode ver todas as configurações do assistente de configuração. Pode efectuar alterações, retrocedendo aos passos anteriores (clique em **Retroceder**).

Se não deseja fazer quaisquer modificações, clique em **Terminar** para finalizar o assistente.

11. Controlo Privacidade

BitDefender monitoriza dezenas de potenciais “hotspots” no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. É bastante eficaz no bloqueio de cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer a sua privacidade e enviar a sua informação pessoal, tal como números de cartão de crédito, do seu computador para o do hacker.

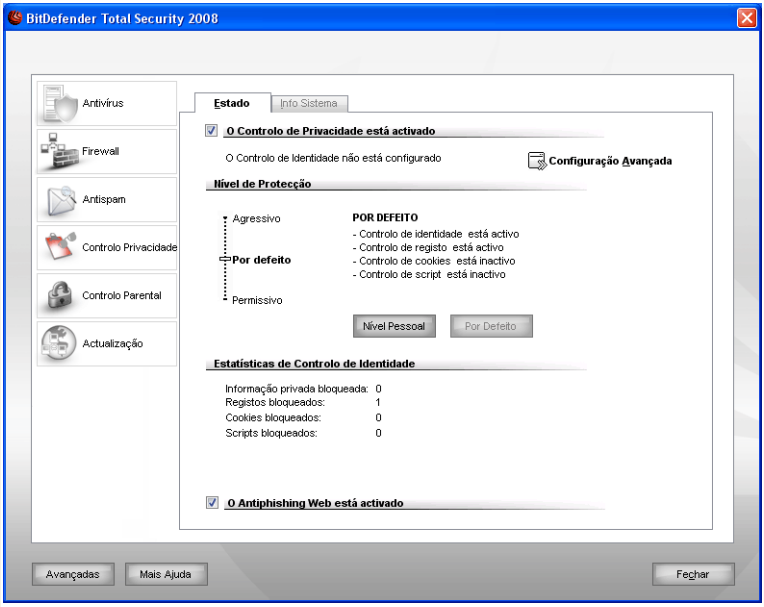
BitDefender também analisa os sites Internet que visita e alerta-o caso seja detectada alguma ameça de phishing.

A secção de **Controlo de Privacidade** deste manual do utilizador contém os seguintes tópicos:

- Estado do Controlo de Privacidade
- Configuração Avançada - Controlo de Identidade
- Configuração Avançada - Controlo de Registo
- Configuração Avançada - Controlo de Cookies
- Configuração Avançada - Controlo de Script
- Informação do Sistema
- Barra de Tarefas Antiphishing

11.1. Estado do Controlo de Privacidade

Para configurar o Controlo de Privacidade e ver informação quanto à sua actividade, clique em **Controlo de Privacidade>Estado** na consola de configuração. A seguinte análise irá aparecer:



Estado do Controlo de Privacidade

11.1.1. Controlo Privacidade

Importante
Para evitar roubo de informação e proteger a sua privacidade mantenha o **Controlo de Privacidade** activado.

O Controlo de Privacidade protege o seu computador usando 5 tipos de controlo de protecção importantes:

- Controlo de Identidade - protege os seus dados confidenciais ao filtrar o tráfego HTTP e SMTP de acordo com as regras que criou na secção de Identidade.

Nota
Ao fundo da secção poderá ver as **Estatísticas do Controlo de Identidade**.

- O Controlo do Registo irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.
- O Controlo de Cookies irá pedir a sua permissão sempre que um novo site web tentar definir um cookie.
- O Controlo de script irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Para definir as configurações para estes controlos clique em Configuração Avançada.

Configurar Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Apenas o **Controlo de Registo** está activo.
Por Defeito	O **Controlo de Registo** e o **Controlo de Identidade** estão activos.
Agressivo	O **Controlo de Registo**, o **Controlo de Identidade** e o **Controlo de Script** estão activos.

Pode personalizar o nível de protecção clicando em **Nível Pessoal**. Na janela que lhe irá aparecer, escolha o controlos de protecção que deseja activar e clique em **OK**.

Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

11.1.2. Protecção Antiphishing

O phishing é uma actividade criminal na Internet que utiliza técnicas maliciosas de forma a enganar as pessoas e levá-las a dar informação considerada privada.

A maior parte das vezes, as tentativas de phishing resumem-se a enviar massivos e-mails que se apresentam como tendo sido enviados por uma empresa legítima e idónea. Estas mensagens enganosas são enviadas com o intuíto de que pelo menos

alguns dos destinatários estejam dentro do perfil que o autor do phishing procura e possam ser persuadidos a divulgar informação considerada privada.

Uma mensagem de phishing normalmente apresenta uma situação que tem a ver com a sua conta online. Tenta convencê-lo a clicar no link que vem na mensagem de forma a que aceda a um suposto site web legítimo (que na verdade trata-se de um site forjado) onde a sua informação privada é solicitada. Poderá, por exemplo, ser solicitada a confirmar a informação da sua conta, tal como a palavra-passe e o utilizador da mesma, e a fornecer o seu número de conta bancária ou o seu número de segurança social. Por vezes, para ser mais convincente, a mensagem indica que a sua conta já foi ou está em vias de ser cancelada se não aceder ao link que vem na mensagem.

O phishing também faz uso do spyware, tais como os Trojan keyloggers, para roubarem a informação bancária directamente do seu computador.

Os principais alvos do phishing são os clientes de pagamento de serviços on-line, tais como o eBay e o PayPal, como também os clientes de bancos que ofereçam serviços online. Recentemente, utilizadores de websites com rede social foram também alvo de phishing com o intuíto de obterem dados de informação pessoal para serem usados para roubo de identidade.

Para estar protegido contra as mais recentes tentativas de phishing quando está a navegar na Internet, mantenha o **Antiphishing** activado. Desta forma, BitDefender irá analisar cada web site antes que lhe aceda e irá alertá-lo da existência de alguma ameaça de phishing. Uma Lista Branca de sites web que não serão analisados pelo BitDefender pode ser configurada.

Ide forma a gerir facilmente a protecção antiphishing e a Lista Branca, use a barra de tarefas do Antiphishing BitDefender que se encontra no integrada no Internet Explorer. Para mais informação, por favor consulte “*Barra de Ferramentas do Antiphishing*” (p. 191).

11.2. Configuração Avançada - Controlo de Identidade

Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações Internet e actualmente fazem-se uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

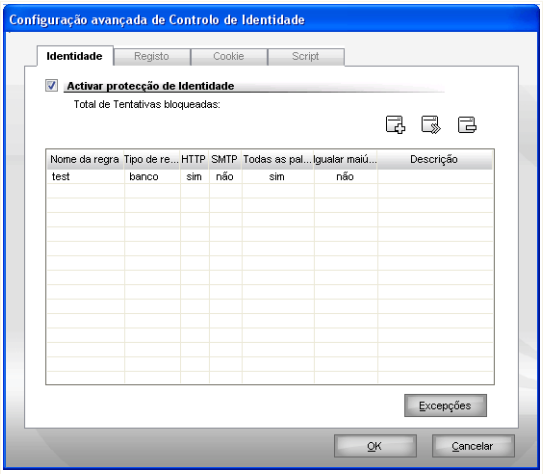
Quer seja o seu e-mail o seu número de cartão de crédito, quandos eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

Controlo de Identidade ajuda-o a manter a sua informação confidencial em segurança. Analisa o tráfego HTTP ou SMTP, ou ambos, em busca de certos caracteres que definiu. Se for encontrada uma correspondência, a respectiva página web ou e-mail são bloqueados.

Suporte multi-utilizador é fornecido de forma a que nenhum utilizador do sistema possa ver as regras que você configurou.

As regras de privacidade podem ser configuradas na secção **Identidade**. Para aceder a esta secção abra a janela **Configuração Avançada de Controlo Privacidade** e clique na barra **Identidade**.

Nota
Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



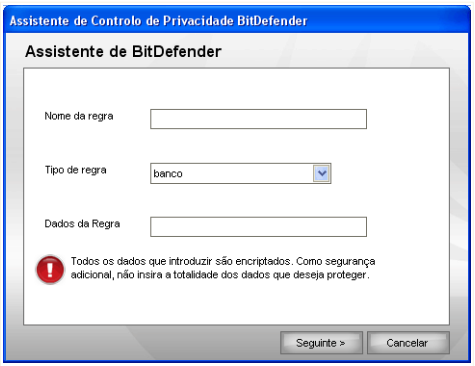
Controlo de Identidade

11.2.1. Criar Regras de Identidade

As regras podem ser introduzidas manualmente (clique no botão **Adicionar** e escolha os parâmetros da regra). O assistente de configuração irá aparecer.

O assistente de configuração é um procedimento composto por 3 passos.

Passo 1/3 - Definir Tipo de Regra e Dados


Assistente de Controlo de Privacidade BitDefender
Assistente de BitDefender
Nome da regra
Tipo de regra
banco
Dados da Regra
Todos os dados que introduzir são encriptados. Como segurança adicional, não insira a totalidade dos dados que deseja proteger.
Seguinte >
Cancelar

Definir Tipo de Regra e Dados

Insira o nome da regra no campo de edição.

Deve definir os seguintes parâmetros:

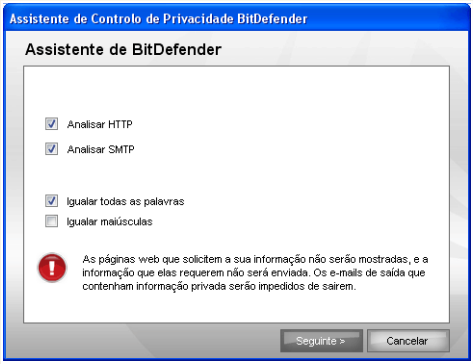
- **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
- **Dados de Regra** - insira os dados da regra.

> ***Nota***
> Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

Clique em **Seguinte**.

Passo 2/3 - Seleccionar Tráfego


Assistente de Controlo de Privacidade BitDefender
Assistente de BitDefender
Analisar HTTP
Analisar SMTP
Igualar todas as palavras
Igualar maiúsculas
As páginas web que solicitem a sua informação não serão mostradas, e a informação que elas requerem não será enviada. Os e-mails de saída que contenham informação privada serão impedidos de sairem.
Seguinte >
Cancelar

Seleccionar Tráfego

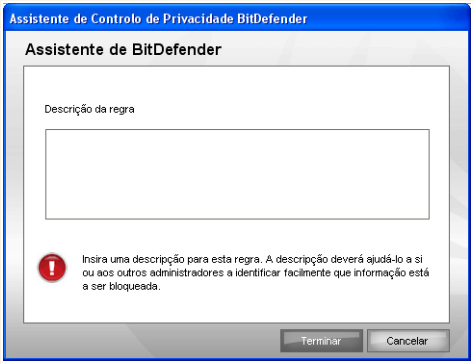
Seleccione o tráfego que quer que o BitDefender analise. Estão disponíveis as seguintes opções:

- **Analisar HTTP** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar SMTP** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

Clique em **Seguinte**.

Passo 3/3 - Descrever Regra


Assistente de Controlo de Privacidade BitDefender
Assistente de BitDefender
Descrição da regra
Insira uma descripção para esta regra. A descripção deverá ajudá-lo a si ou aos outros administradores a identificar facilmente que informação está a ser bloqueada.
Terminar
Cancelar

Descrever Regra

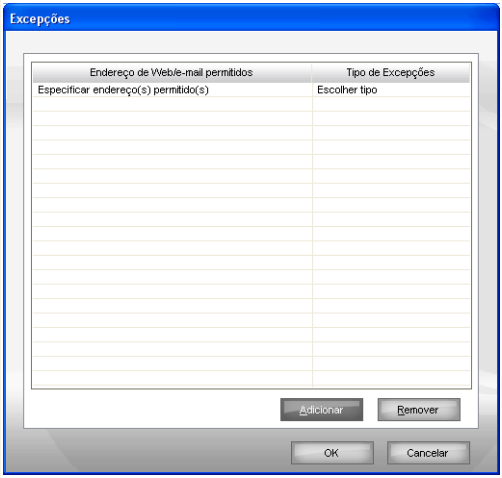
Insira uma breve descrição da regra no campo de edição.

Clique em **Terminar**.

11.2.2. Definir Excepções

Há casos em que necessita de definir excepções para especificar as regras de identidade. Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde pode gerir as excepções, clique em **Excepções**.



Excepções

Para adicionar uma excepção, siga os seguintes passos:

1. Clique **Adicionar** para adicionar uma nova entrada na lista.
2. Duplo-clique em **Especificar endereço permitido** e inserir o endereço web ou endereço de e-mail que deseja adicionar como excepção.
3. Duplo-clique em**Escolher Tipo** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione**SMTP**.

Para remover uma excepção da lista, seleccione-a e clique **Remover**.

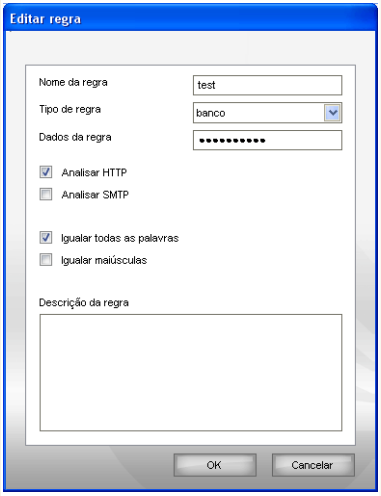
Clique em **OK** para guardar as alterações.

11.2.3. Gerir Regras

Pode ver as regras listadas na tabela.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para desactivar temporariamente uma regra sem a apagar, limpe a caixa de selecção correspondente.

Para editar uma regra, seleccione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.



Editar Regra

Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

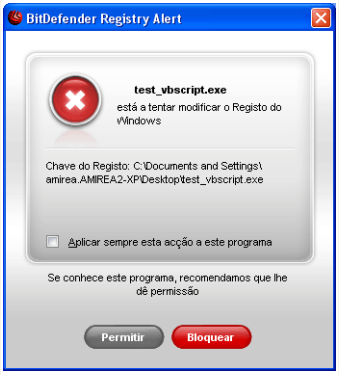
Clique em **OK** para guardar as alterações e fechar a janela.

11.3. Configuração Avançada - Controlo de registo

Uma parte muito importante do sistema operativo do Windows é chamado de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí fora.

O **Registo** também é utilizado para definir quais os programas que deverão ser lançados automaticamente ao iniciar o Windows. Frequentemente, os vírus usam isto para se lançarem automaticamente quando o utilizador reiniciar o seu computador.

O **Controlo de registo** vigia o Registo do Windows – mais uma vez, isto é útil para detectar Cavalos de Tróia. Irá alertá-lo sempre que um programa tente modificar uma entrada de registo para poder ser executado ao iniciar o Windows.


BitDefender Registry Alert
test_vbscript.exe
está a tentar modificar o Registo do Windows
Chave do Registo: C:\Documents and Settings\amirea.AMIREA2-XP\Desktop\test_vbscript.exe
Aplicar sempre esta acção a este programa
Se conhece este programa, recomendamos que lhe dê permissão
Permitir
Bloquear

Alerta de registo

Pode negar esta modificação ao clicar em **Não** ou pode permitir ao clicar em **Sim**.

Se deseja que o BitDefender memorize a sua resposta tem de seleccionar a caixa de selecção: **Aplicar sempre esta acção a este programa**. Desta forma, uma regra será criada e a mesma acção será aplicada sempre que este programa tente modificar uma entrada no registo de forma a ser executado no iniciar do Windows.

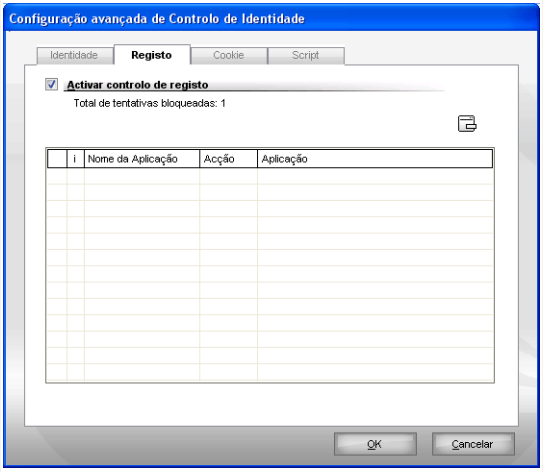
Nota

O BitDefender irá, normalmente, alertá-lo quando instalar novos programas que necessitem de se executar durante o iniciar do seu computador. Na maioria dos casos, estes programas são legítimos e de confiança.

Cada regra que foi memorizada pode ser acedida na secção **Registo** para futura afinação. Para aceder a esta secção abrir a janela**Configuração Avançada de Controlo de Privacidade**e clique na barra**Registo**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



Controlo de Registo

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para temporariamente desactivar uma regra sem a apagar, deseleccione a respectiva caixa de selecção.

Para alterar a acção de uma regra,, faça duplo-clique do campo da acção e seleccione a opção correspondente do menu.

Clique em **OK** para fechar a janela.

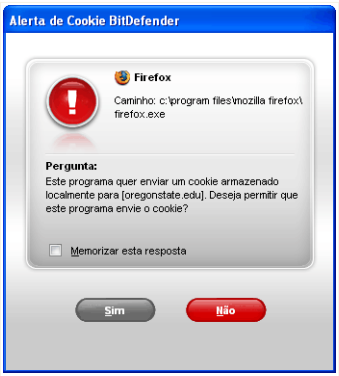
11.4. Configuração Avançada - Controlo de Cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros pequenos armazenados no seu computador. Os sites da Web criam estas cookies para manter um rasto de informação específica sobre si.

As Cookies são geralmente criadas para facilitar a sua vida. Por exemplo, elas podem ajudar o site da Web a lembrar-se do seu nome e preferências, para que não tenha de os voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto do seu padrão de navegação.

É aqui que o **Controlo de Cookies** ajuda. Quando activo, o **Controlo de Cookies** irá pedir a sua permissão sempre que um site da web tentar estabelecer uma cookie:


Alerta de Cookie BitDefender
Firefox
Caminho: c:\program files\mozilla firefox\firefox.exe
Pergunta:
Este programa quer enviar um cookie armazenado localmente para [oregonstate.edu]. Deseja permitir que este programa envie o cookie?
Memorizar esta resposta
Sim
Não

Alerta de Cookie

Pode ver o nome da aplicação que está a tentar enviar um ficheiro de cookie.

Seleccione **Memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando se ligar ao mesmo site.

Isto irá ajudá-lo a escolher quais os sites da web em que pode confiar ou não.

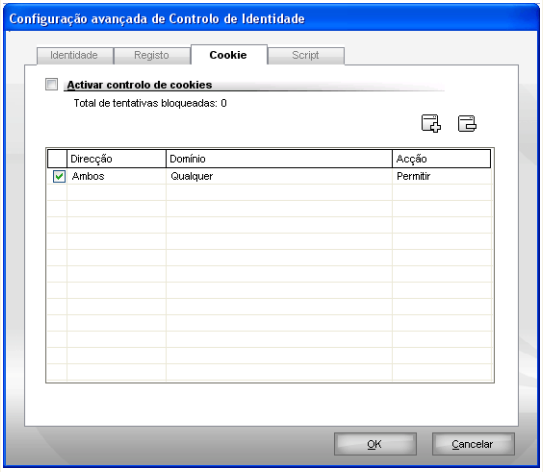
Nota

Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido de início. Inicialmente, irá perguntar uma série de questões acerca de sites que tentam colocar cookies no seu computador. Logo que adicione os seus sites habituais à lista de regras, a navegação tornar-se-á tão fácil como antes.

Toda a regra que foi memorizada pode ser acedida na secção **Cookies** para uma maior afinação. Para aceder a esta secção, abra a janela **AConfiguração Avançada do Controlo de Privacidade** e clique na barra**Cookie**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



Controlo de Cookies

Pode ver as regras criadas até agora listadas na tabela.

Importante
A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

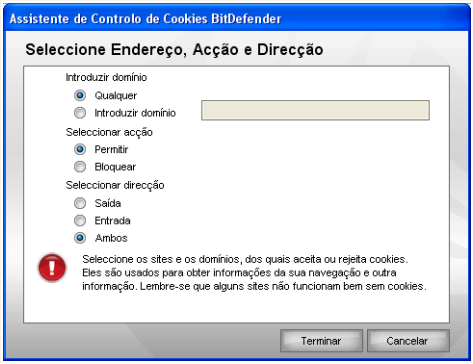
Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

11.4.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço, Acção e Direcção


Assistente de Controlo de Cookies BitDefender
Seleccione Endereço, Acção e Direcção
Introduzir domínio
Qualquer
Introduzir domínio
Seleccionar acção
Permitir
Bloquear
Seleccionar direcção
Saída
Entrada
Ambos
Seleccione os sites e os domínios, dos quais aceita ou rejeita cookies. Eles são usados para obter informações da sua navegação e outra informação. Lembre-se que alguns sites não funcionam bem sem cookies.
Terminar
Cancelar

Seleccionar Endereço, Acção e Direcção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os cookies desse domínio serão executados.
Bloquear	Os cookies desse domínio não serão executados.

- **Sentido** - selecciona o sentido do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas às cookies que são enviadas para fora para o site a que está ligado.
Entrada	A regra será aplicada apenas às cookies que são recebidas do site a que está ligado.
Ambos	A regra aplica-se em ambos os sentidos.

Clique em **Terminar**.

Nota
Pode aceitar cookies sem nunca as devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

Clique em **OK** para guardar as alterações e fechar a janela.

11.5. Configuração Avançada - Controlo de Script

Scripts e outros códigos tais como Controlos de ActiveX e Java applets, os quais são usados para criar páginas da web interactivas, podem ser programados para ter efeitos nocivos. Os elementos do ActiveX, por exemplo, podem ganhar total acesso aos seus dados e podem ler dados do seu computador, informação eliminada, capturar palavras-passe e interceptar mensagens enquanto está ligado. Apenas deverá aceitar conteúdo activo de sites que conhece e confia totalmente.

BitDefender deixa-o escolher entre permitir ou bloquear a execução destes elementos.

Com o **Controlo de script** terá a seu cargo escolher os sites da web, nos quais confia ou não. O BitDefender irá pedir a sua permissão sempre que um site da web tente activar um script ou outro conteúdo activo:

Alerta de Script BitDefender
Firefox
Caminho: c:\program files\mozilla firefox\firefox.exe
Pergunta:
Este programa recebeu conteúdo activo (ActiveX/Java Applet/Script) de [gramos.wordpress.com] através do serviço http. Deseja que permitir que este programa o armazene no seu pc?
Memorizar esta resposta
Sim
Não

Alerta de Script

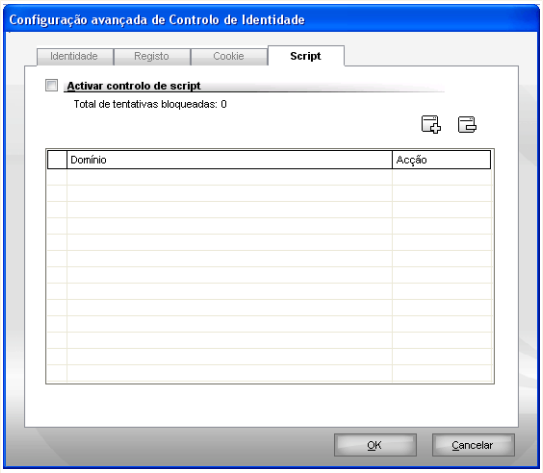
Pode ver o nome do recurso.

Seleccione **memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando o mesmo site tentar enviar-lhe conteúdo activo.

Toda a regra que foi memorizada pode ser acedida na secção **Script** para futura afinação. Para aceder a esta secção, abra a janela**Configuração Avançada do Controlo de Privacidade** e clique na barra**Script**.

Nota

Para abrir a janela **Configuração Avançada de Controlo Privacidade** clique em **Controlo Privacidade>Estado** na consola de configuração e clique em **Configuração Avançada** .



Controlo de script

Pode ver as regras criadas até agora listadas na tabela.

Importante

A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

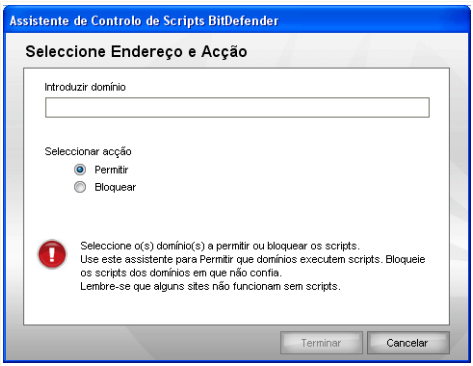
Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

11.5.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço e Acção


Assistente de Controlo de Scripts BitDefender
Seleccione Endereço e Acção
Introduzir domínio
Seleccionar acção
Permitir
Bloquear
Seleccione o(s) domínio(s) a permitir ou bloquear os scripts.
Use este assistente para Permitir que domínios executem scripts. Bloqueie os scripts dos domínios em que não confia.
Lembre-se que alguns sites não funcionam sem scripts.
Terminar
Cancelar

Seleccionar Endereço e Acção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os scripts desse domínio serão executados.
Bloquear	Os scripts desse domínio não serão executados.

Clique em **Terminar**.

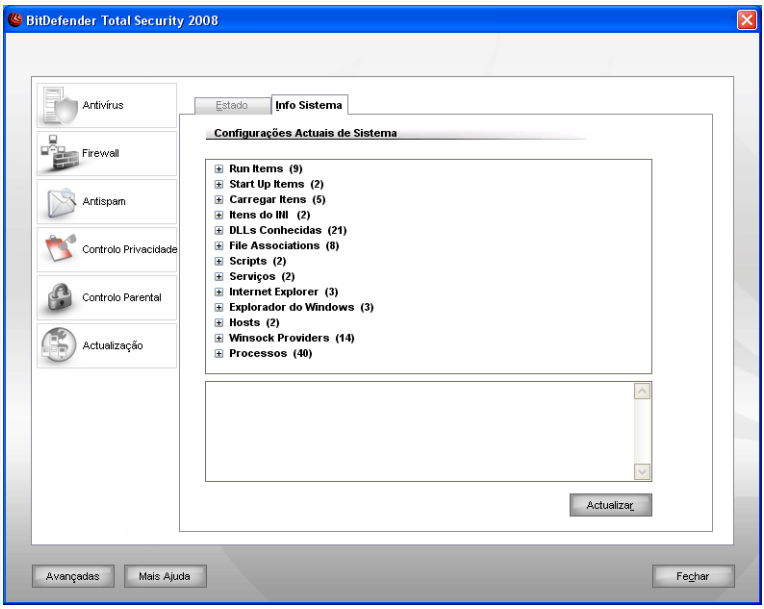
Clique em **OK** para guardar as alterações e fechar a janela.

11.6. Info do Sistema

BitDefender permite-lhe visualizar, a partir de uma única localização, todas as configurações do sistema e as aplicações registadas para se executarem durante o

iniciar do Windows. Desta forma, pode gerir a actividade da seu sistema e as aplicações instaladas nele como também identificar possíveis infecções.

Para obter a informação do sistema, clique em **Controlo de Privacidade>Info Sistema** na consola de configuração. A seguinte análise irá aparecer:



Info do Sistema

A lista contém todos os itens carregados quando inicia o sistema assim como os itens carregados pelas diferentes aplicações.

Estão disponíveis três botões:

- **Remover** - apaga o item seleccionado. Tem de clicar em **Sim** para confirmar a sua escolha.

Nota
Se não deseja ser mais notificado novamente para confirmar a sua escolha durante a actual sessão, seleccione **Não me questionem mais durante esta sessão**.

- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).
- **Actualizar** - reabre a secção de **Info Sistema**.

Nota
Dependendo do item seleccionado, um ou ambos os botões **Remover** ou **Ir Para** poderão não aparecer.

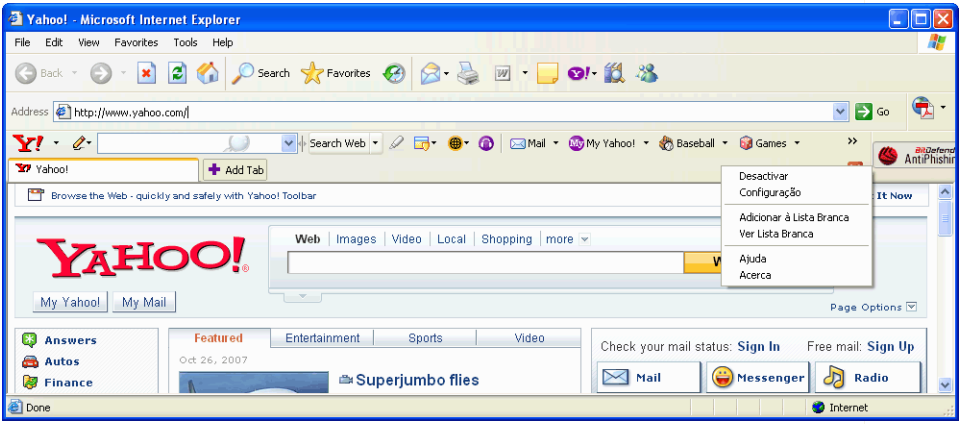
11.7. Barra de Ferramentas do Antiphishing

BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet. Analisa os sites web que acede e alerta-o no caso de haver alguma ameaça de phishing. Uma Lista Branca de sites web que não serão analisados pelo BitDefender pode ser configurada.

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada no Internet Explorer.

A barra de ferramentas antiphishing representado pelo **icone do BitDefender**, está localizado no lado superior da Internet Explorer. Clique nele de forma a abrir o menu da barra de ferramentas.

Nota
Se não consegue ver a barra de ferramentas, abra o menu **Ver** siga para **Barras de ferramentas** e seleccione **Barra de Ferramentas BitDefender**.



Barra de Ferramentas do Antiphishing

Os seguintes comandos estão disponíveis no menu da barra de ferramentas:

- **Activar/Desactivar** - activa/desactiva a barra de ferramentas Antiphishing do BitDefender.

  Nota
  Se escolher desactivar a a barra de ferramentas antiphishing, não ficará mais protegido contra as tentativas de phishing.

- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing.

  Estão disponíveis as seguintes opções:
  - **Activar Análise** - activa a análise antiphishing.
  - **Avisar antes adicionar à lista branca** - será consultado antes de ser adicionado um site web à Lista Branca.
- **Adicionar à Lista Branca** - adiciona o actual site web à Lista Branca.

  Nota
  Adicionar um site à Lista Branca significa que o BitDefender não irá mais analisar esse site em busca de tentativas de phishing. Recomendamos que adicione à Lista Branca apenas os sites em que confia totalmente.

- **Ver Lista Branca** - abre a Lista Branca.

Pode ver toda a lista dos sites web que não estão a ser analisados pelos motores de antiphishing do BitDefender.

Se deseja remover um site da Lista Branca de forma a que seja notificado acerca de qualquer possibilidade de ameaça de phishing existente nesse site, clique no botão **Remover** ao pé do mesmo.

Pode adicionar sites à Lista Branca nos quais confia absolutamente, de forma a que eles não sejam mais analisados pelos motores antiphishing. Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

- **Ajuda**- abre o ficheiro de ajuda.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

12. Controlo Parental

O Controlo Parental pode bloquear o acesso a:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- páginas wen e mensagens de e-mail que contenham determinadas palavras-chave.
- aplicações tais como: jogos, programas de partilha de ficheiros e outros.

Importante
Este módulo só pode ser acedido e configurado por utilizadores com direitos de administrador (administradores de sistema). Se as configurações estão protegidas por palavra-passe, só podem ser modificadas se a palavra-passe for inserida. Um administrador não pode impôr um conjunto de regras a um utilizador para o qual as regras foram previamente definidas por outro administrador.

A secção de **Controlo Parental** deste manual do utilizador contém os seguintes tópicos:

- Proteger as Definição do Controlo Parental
- Estado do Controlo Parental
- Controlo Web
- Controlo de aplicações
- Filtragem por Palavra-chave
- Temporizador Web

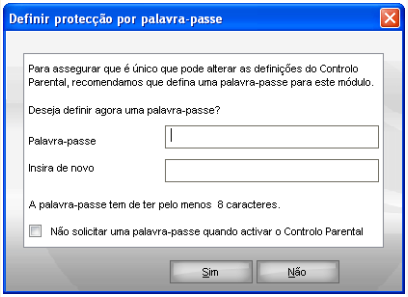
12.1. Proteger as Definições do Controlo Parental

Se não for a única pessoa com direitos administrativos a utilizar este computador, recomendamos que protega as suas configurações do Controlo Parental com uma palavra-passe. Ao definir uma palavra-passe, irá prevenir que outros utilizadores com direitos administrativos possam mudar as suas definições do Controlo Parental que configurou para um determinado utilizador.

BitDefender irá solicitar-lhe por defeito que defina uma palavra-passe quando activar o Controlo Parental.

Para definir protecção por palavra-passe, faça o seguinte:

1. Digite a palavra-passe na campo **Palavra-passe** .
2. Insira de novo a palavra-passe no campo **Reinserir Palavra-passe** para a confirmar.
3. Clique em **OK** para guardar a palavra-passe e fechar a janela.


Definir protecção por palavra-passe
Para assegurar que é único que pode alterar as definições do Controlo Parental, recomendamos que defina uma palavra-passe para este módulo.
Deseja definir agora uma palavra-passe?
Palavra-passe
Insira de novo
A palavra-passe tem de ter pelo menos 8 caracteres.
Não solicitar uma palavra-passe quando activar o Controlo Parental
Sim
Não

Definir Protecção por Palavra-passe

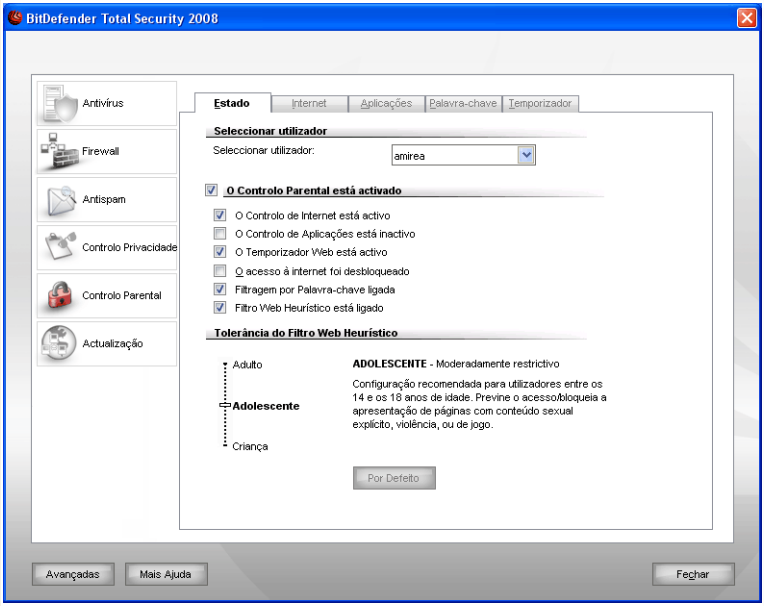
Uma vez definida a palavra-passe, se desejar modificar as definições do Controlo Parental, ser-lhe-á pedido que insira a palavra-passe. Os outros administradores de sistema (se existirem) terão também de inserir a palavra-passe de forma a poderem alterar as definições do Controlo Parental.

Nota
A palavra-passe não protege quaisquer outras definições do BitDefender.

Caso não defina uma palavra-passe e não queira que a janela para o efeito lhe surja novamente, seleccione **Não solicitar palavra-passe quando activar Controlo Parental**.

12.2. Estado do Controlo Parental

Para configurar o Controlo Parental para um determinado utilizador, clique em **Controlo Parental>Estado** na consola de configuração. A seguinte análise irá aparecer:



Estado do Controlo Parental

Importante
Mantenha o **Controlo Parental** activado de forma a proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.

12.2.1. Seleccionar Controlo de Protecção

De forma a configurar o nível de protecção deve em primeiro lugar seleccionar o utilizador ao qual deseja aplicar essas configurações. Depois configure o nível de protecção usando os seguintes controlos:

- **Controlo Web** - activa o**Controlo Web** de forma a filtrar a navegação na Internet de acordo com as regras definidas por si na secção Web .
- **Controlo de Aplicações** - activa o **Controlo de Aplicações** de forma a bloquear o acesso às aplicações no seu computador de acordo com as regras definidas por si na secçãoAplicações.

- **Temporizador Web** - activa o **Temporizador Web** de forma a permitir o acesso à web de acordo com a tabela de horário definida por si na secçãoTemporizador .
- **Acesso Web** - activa esta opção de forma a bloquear o acesso a todos os websites (não só apenas aqueles definidos na secção Web).
- **Filtragem Palavra-chave** - activa a **Filtragem Palavra-chave** de forma a filtrar o acesso à web e o ao correio electrónico de acordo com as regras definidas por si na secçãoPalavra-chave .
- **Filtro web Heurístico** - activa esta opção de forma a filtrar o acesso à web de acordo com regras pré-estabelecidas baseadas em categorias de idade.

Nota

De forma a tirar o máximo benefício das características oferecidas pelo Controlo Parental, deve de configurar os controlos seleccionados. Para aprender como configurá-los, por favor consulte os seguintes tópicos deste capítulo.

12.2.2. Configurar Filtro Web Heurístico

O filtro web heurístico analisa as páginas web e bloqueia aquelas que correspondem aos modelos de conteúdos potencialmente inapropriados.

De forma a filtrar o acesso à web de acordo com um conjunto de regras (ruleset) de idade, deverá definir um determinado nível de tolerância. Arraste o marcador ao longo da escala para definir o nível de tolerância que considera apropriado para o utilizador seleccionado.

Existem 3 níveis de tolerância:

Nível de Tolerância	*Descrição*
Criança	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para utilizadores menores de 14. São bloqueadas as páginas web com um potencial conteúdo prejudicial para as crianças (porno, sexualidade, drogas, hacking, etc.).
Adolescente	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para utilizadores entre os 14 e os 18 anos de idade. São bloqueadas as páginas web com um conteúdo sexual, pornográfico ou adulto.

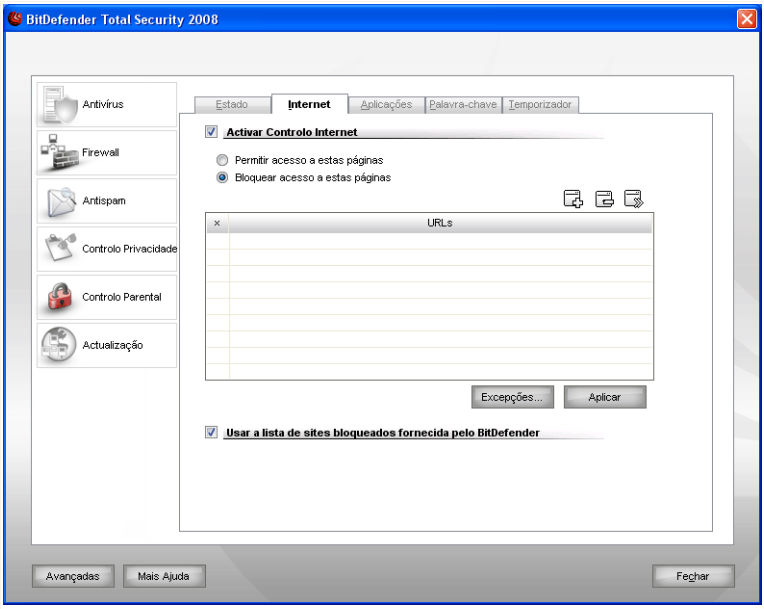
Nível de Tolerância	Descrição
Adulto	Oferece um acesso sem restrições a todas as páginas web independentemente do seu conteúdo.

Clique em **Nível por Defeito** para colocar o marcador no nível por defeito.

12.3. Controlo Web

O **Controlo Web** ajuda-o a bloquear o acesso a web sites com conteúdo inapropriado. Uma lista de candidatos a serem bloqueados, quer sites quer partes dos mesmos, é fornecida e actualizada pelo BitDefender, como parte do processo normal de actualização.

Para configurar o Controlo Web, clique em **Controlo Parental>Web** na consola de configuração. A seguinte análise irá aparecer:



Controlo Web

Para activar esta protecção seleccione a caixa de selecção correspondente a **Activar Controlo Internet**.

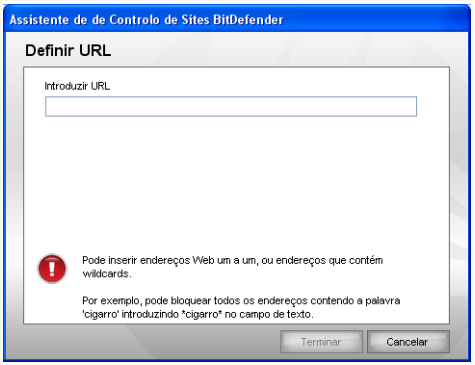
Seleccione **Permitir acesso a estas páginas**/**Bloquear acesso a estas páginas** para ver a lista dos sites permitidos/bloqueados. Clique em **Excepções...** para aceder à janela onde pode ver a lista complementar.

As regras devem ser inseridas manualmente. Primeiro que tudo, seleccione **Permitir acesso a estas páginas**/**Bloquear acesso a estas páginas** para permitir/bloquear o acesso aos sites web que irá especificar no assistente. Então clique no botão **Adicionar...** para iniciar o assistente de configuração.

12.3.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Especificar sites web


Assistente de de Controlo de Sites BitDefender
Definir URL
Introduzir URL
Pode inserir endereços Web um a um, ou endereços que contém wildcards.
Por exemplo, pode bloquear todos os endereços contendo a palavra 'cigarro' introduzindo *cigarro* no campo de texto.
Terminar
Cancelar

Especificar Sites Web

Introduza o site web para o qual a regra será aplicada e clique em **Terminar**.

Importante
Sintaxe:

- `*.xxx.com` - a acção da regra será aplicada a todos os sites web que terminam em `.xxx.com`;
- `*porn*` - a acção da regra será aplicada a todos os sites web que contenham `porn` no endereço do site web;

- `www.*.com` - a acção da regra será aplicada a todos os sites web que tenham o sufixo de domínio `com`;
- `www.xxx.*` - a acção da regra será aplicada a todos os sites web que comecem por `www.xxx.` sem importar o sufixo do domínio.

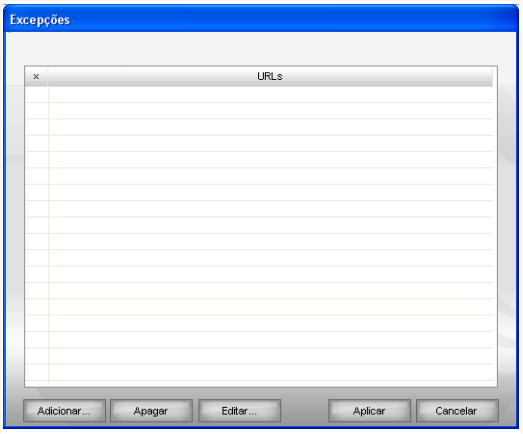
Clique em **Aplicar** para guardar as alterações.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para modificar uma regra seleccione-a e clique no botão **Editar...** ou faça duplo-clique sobre ela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

12.3.2. Especificar Excepções

Por vezes necessita de especificar excepções para uma regra em particular. Por exemplo, define uma regra que bloqueia sites que contêm a palavra "hard" no endereço (sintaxe: `*hard*`). Também está consciente da existência de um site denominado `hard-rock` onde os visitantes podem ouvir música on-line. Para abrir uma excepção à regra previamente criada, aceda à janela **Excepções** e defina uma excepção para a regra.

Clique em **Excepções...**. A seguinte janela irá aparecer:



Especificar Excepções

Clique em **Adicionar...** para especificar excepções. O assistente de configuração aparecerá. Complete o assistente de forma a definir a excepção.

Clique em **Aplicar** para guardar as alterações.

Para apagar uma regra, apenas seleccione-a e clique em **Apagar**. Para modificar uma regra seleccione-a e clique em **Editar...** ou faça um duplo-clique nela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

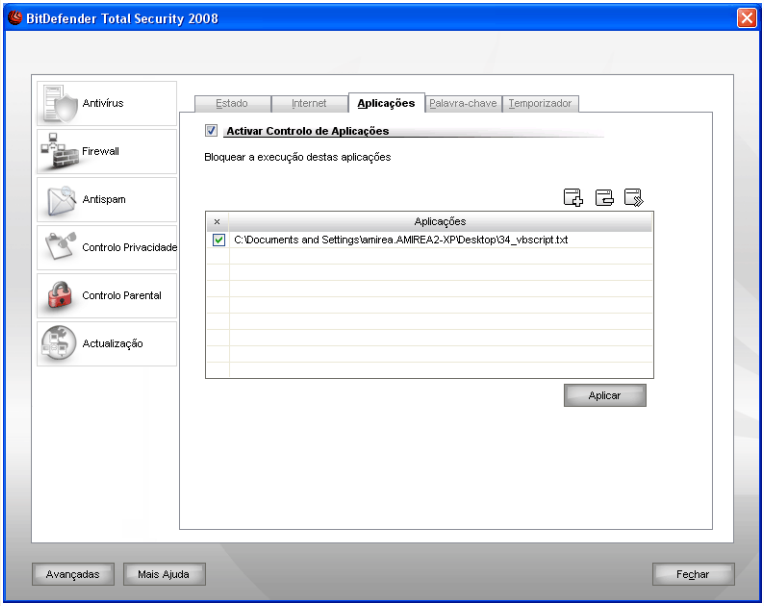
12.3.3. Lista Negra Web BitDefender

De forma a proteger as suas crianças, o BitDefender dá-lhe um lista negra de sites web com conteúdo inapropriado ou possivelmente perigoso. Para bloquear os sites que aparecem nesta lista seleccione **Usar a lista dos sites bloqueados fornecidos por BitDefender**.

12.4. Controlo de aplicações

O **Controlo de aplicações** ajuda-o a bloquear qualquer programa impedindo-o de se executar. Jogos, software de multimédia e de mensagens, assim como outras categorias de software e malware podem ser bloqueados desta forma. As aplicações bloqueadas desta forma ficam também protegidas contra modificações, e não podem ser copiadas ou movidas.

para configurar o Controlo de Aplicações, clique em **Controlo Parental>Aplicações** na consola de configuração. A seguinte análise irá aparecer:



Controlo de aplicações

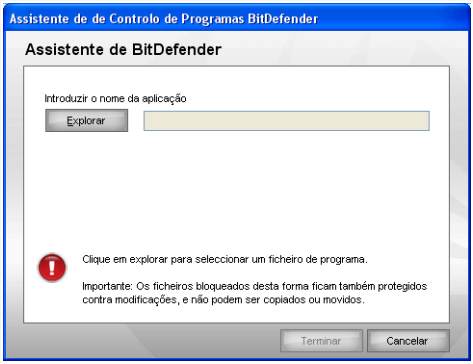
Para activar esta protecção seleccione a caixa de selecção correspondente para **Activar Controlo de Aplicações**.

As regras devem ser inseridas manualmente. Clique no botão **Adicionar...** para dar início ao assistente de configuração.

12.4.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Aplicação a Bloquear


Assistente de Controlo de Programas BitDefender
Assistente de BitDefender
Introduzir o nome da aplicação
Explorar
Clique em explorar para seleccionar um ficheiro de programa.
Importante: Os ficheiros bloqueados desta forma ficam também protegidos contra modificações, e não podem ser copiados ou movidos.
Terminar
Cancelar

Seleccionar Aplicação a Bloquear

Clique em **Explorar**, seleccione a aplicação a ser bloqueada e clique em **Terminar**.

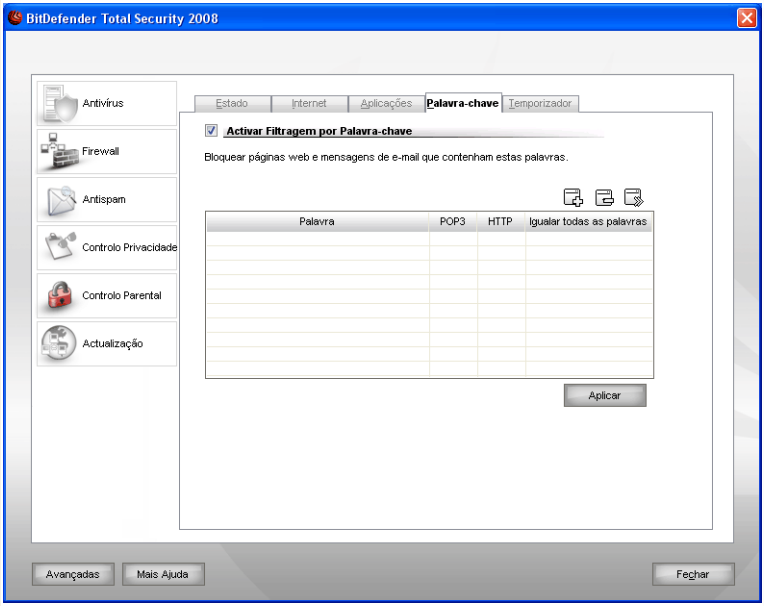
Clique em **Aplicar** para guardar as alterações.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para modificar uma regra seleccione-a e clique no botão **Editar...** ou faça duplo-clique sobre ela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

12.5. Filtragem Palavra-chave

O **Filtro palavra-chave** ajuda-o a bloquear o acesso a mensagens de e-mail ou a páginas web que contenham uma palavra específica. Desta forma poderá impedir que os utilizadores vejam palavras ou frases inapropriadas.

Para configurar o Filto Palavra-Chave, clique em **Controlo Parental>Palavra-chave** na consola de configuração. A seguinte análise irá aparecer:



Filtragem Palavra-chave

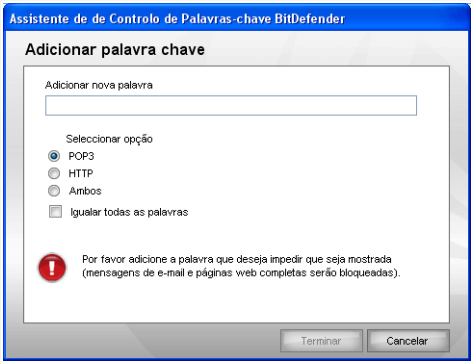
Para activar esta protecção seleccione a caixa de selecção correspondente a **Filtragem palavra-chave**.

As regras devem ser inseridas manualmente. Clique no botão **Adicionar...** para dar início ao assistente de configuração.

12.5.1. Assistente de Configuração

O assistente de configuração é um procedimento de 1 passo.

Passo 1/1 - Inserir Palavra-chave


Assistente de de Controlo de Palavras-chave BitDefender
Adicionar palavra chave
Adicionar nova palavra
Seleccionar opção
POP3
HTTP
Ambos
Igualar todas as palavras
Por favor adicione a palavra que deseja impedir que seja mostrada (mensagens de e-mail e páginas web completas serão bloqueadas).
Terminar
Cancelar

Inserir Palavra-chave

Deve definir os seguintes parâmetros:

- **Palavra-chave** - insira no campo de edição a palavra ou frase que deseja bloquear.
- **Protocolo** - escolha o protocolo que o BitDefender deve analisar para a palavra especificada.

  Estão disponíveis as seguintes opções:

Opção	Descrição
POP3	As mensagens de e-mail que contenham a palavra-chave são bloqueadas.
HTTP	As páginas web que contenham a palavra-chave são bloqueadas.
Ambos	As mensagens de e-mail e as páginas web que contenham a palavra-chave serão bloqueadas.

Clique em **Aplicar** para guardar as alterações.

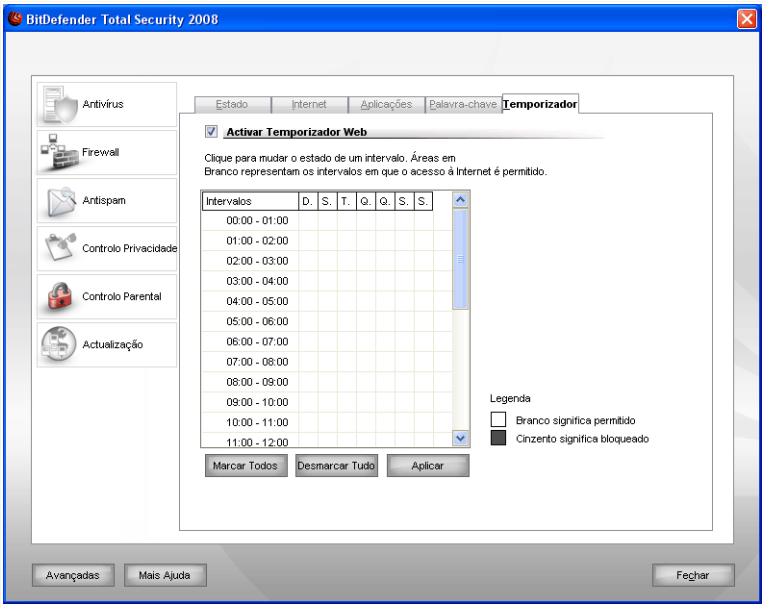
Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para modificar uma regra seleccione-a e clique no botão **Editar...** ou faça duplo-clique sobre ela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

12.6. Temporizador Web

O **Temporizador Web** ajuda-o a permitir ou bloquear acessos à web por parte dos utilizadores ou aplicações durante determinados intervalos de tempo.

Nota
O BitDefender efectuará a actualização de hora-a-hora independentemente da configuração do **Temporizador Web**.

Para configurar o Temporizador Web, clique em **Controlo Parental>Temporizador** na consola de configuração. A seguinte análise irá aparecer:



Temporizador Web

Para activar esta protecção seleccione a caixa de selecção correspondente a **Activar Temporizador Web**.

Seleccione os intervalos de tempo em que todas as ligações à Internet estarão bloqueadas. Pode clicar em células individuais ou pode clicar e arrastar o ponteiro

de forma a cobrir longos períodos de tempo. Também pode clicar em **Marcar Todas** para seleccionar todas as células, implicitamente, bloqueando todo o acesso à web. Se clicar em **Desmarcar Todas**, as ligações de internet serão sempre permitidas.

Importante
As células coloridas a cinzento representam intervalos de tempo em que as ligações à Internet estão bloqueadas.

Clique em **Aplicar** para guardar as alterações.

13. Actualização

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o BitDefender executa esta operação sozinho. Quando liga o computador o BitDefender verifica se há novas actualizações e depois disso fá-lo a cada **hora** .

Se uma actualização for detectada, dependendo das opções definidas na secção Definições da Actualização Automática, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

As actualizações existem nas seguintes formas:

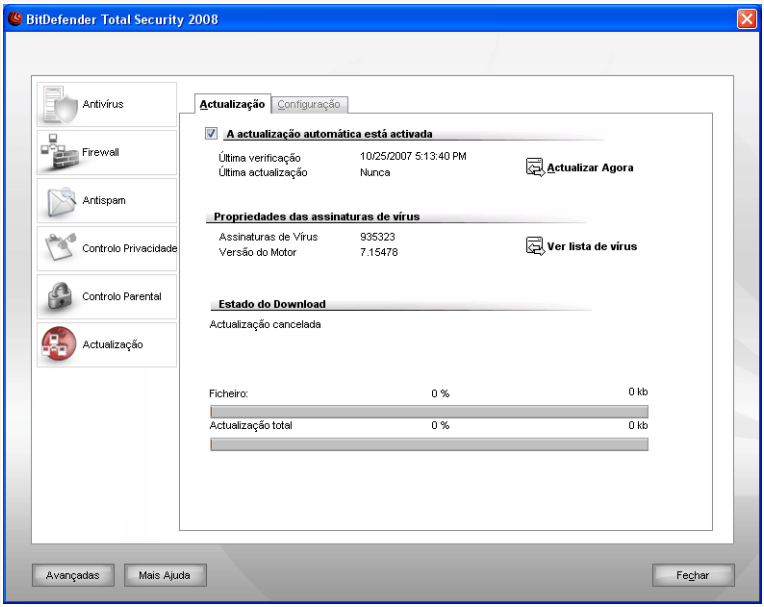
- **Actualizações do motor antivírus** - à medida que surgem novas ameaças, os ficheiros que contêm as assinaturas de vírus têm de ser actualizados para assegurar uma protecção permanentemente actualizada contra elas. Esta actualização também é conhecida como **Actualização das Definições de Vírus**.
- **Actualizações do motor Antispam** - novas regras serão adicionadas ao Filtro Heurístico e ao Filtro URL e novas imagens serão adicionadas ao Filtro de Imagem. Isto irá a judar a melhorar a eficácia do seu motor Antispam. Esta actualização é também conhecida como **Actualização Antispam**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Actualização Antispyware**.
- **Upgrades do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de análise, com o objectivo de melhorar o desempenho do produto. Esta actualização também é conhecida como **Mudança de Versão**.

A secção de **Actualização** deste guia do utilizador contém os seguintes tópicos:

- Actualização Automática
- Configurações da Actualização

13.1. Actualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** na consola de configuração. A seguinte análise irá aparecer:



Actualização Automática

Aqui poderá ver quando foi feita a última actualização e a última verificação de actualizações, com também a informação da última actualização feita (se bem-sucedida, se ocorreram erros). Também a informação acerca da versão do motor e o número de assinatura são mostrados.

Pode obter as assinaturas de malware do seu BitDefender ao clicar **Mostrar Lista de Vírus**. Um ficheiro HTML que contém todas as assinaturas disponíveis será criado e aberto no browser da internet. Pode procurar uma assinatura específica de malware por entre a base de dados ou clicar **Lista de Vírus BitDefender** para aceder à base de dados de assinaturas BitDefender on-line.

Se abrir esta secção durante uma actualização, poderá o estado do download.

Importante
Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

13.1.1. Solicitar uma Actualização

A actualização automática pode ser feita a qualquer altura que deseje clicando no botão **Actualizar Agora**. Esta actualização é também conhecida como **Actualização a pedido do utilizador**.

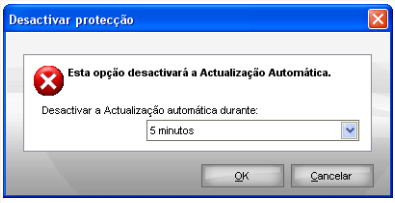
O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça o quanto antes.

Nota
Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

13.1.2. Desactivar Actualização Automática

Se deseja desactivar a actualização automática, uma janela de aviso aparecerá.



Desactivar Actualização Automática

Tem de confirmar a sua escolha ao seleccionar no menu durante quanto tempo deseja que a actualização automática fique desactivada. Pode desactivar a actualização

automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

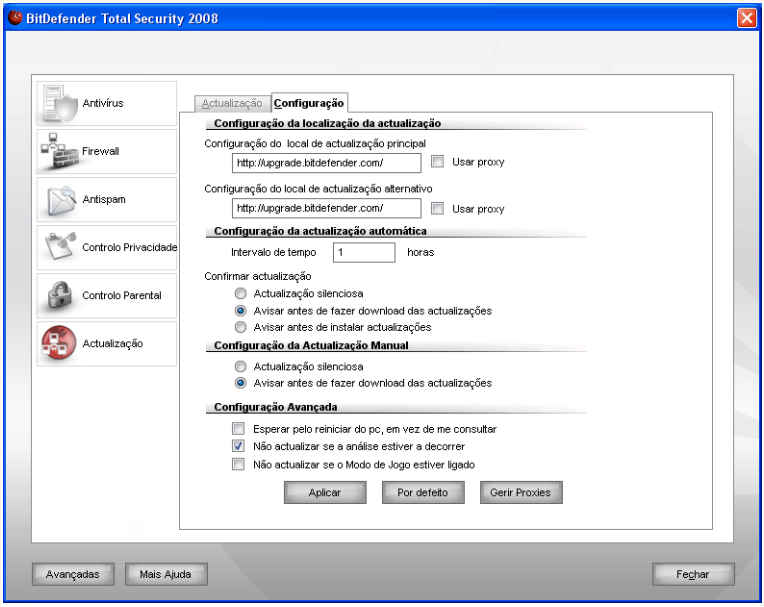
Atenção

Esta é uma incidência de segurança critica. recomendamos que desactive a actualização automática pelo menor tempo possível. Se o BitDefender não for actualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

13.2. Definições de actualização

As actualizações podem ser executadas através da rede local, da Internet, directamente ou através de um servidor proxy. Por defeito, o BitDefender verificará as actualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

Para configurar as definições de actualização e gerir proxies, clique em **Actualização>Configuração** na consola de configuração. A seguinte análise irá aparecer:



Definições de actualização

As configurações da actualização estão agrupadas em 4 categorias (**Configuração da Localização da Actualização**, **Configuração de actualização automática**, **Configuração de Actualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.

13.2.1. Configuração da Localização da Actualização

Para definir a localização da actualização, use as opções da categoria **Configuração da Localização da Actualização** .

Nota
Configure estas definições apenas se estiver ligado a uma rede local que armazena localmente as assinaturas de malware do BitDefender ou se liga à Internet através de um servidor proxy.

Para actualizações mais rápidas e fiáveis, pode configurar dois locais de actualização: um **Local primário de actualização** e um **Local alternativo de actualização**. Por defeito estas localizações são iguais:`http://upgrade.bitdefender.com`.

Para modificar um dos locais de actualização, insira o URL do local mirror no campo **URL** que corresponde ao novo local para o qual deseja mudar.

Nota
Recomendamos que defini como local primário de actualização o local mirror e deixar o local alternativo de actualização como está, como um plano de backup em caso do local mirror ficar indisponível.

No caso em que a empresa usa um servidor proxy para se ligar à Internet, seleccione **Usar proxy** de depois clique em **Gerir proxies** para configurar as definições do proxy.

Nota
Para mais informação, por favor consulte "*Gerir Proxies*" (p. 214)

13.2.2. Configurar Actualização Automática

Para configurar o processo de actualização automática do BitDefender, use as opções na categoria **Configuração Actualização Automática** .

Pode definir o intervalo entre duas verificações consecutivas de actualizações no campo **Interval Tempo**. Por defeito, o intervalo de tempo da actualização é de 1 hora.

Para definir como é que o processo de actualização automática tem de ser feito, seleccione uma das seguintes opções:

- **Actualização silenciosa** - O BitDefender faz automaticamente o download e a implementação da actualização.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.

Nota
Será avisado antes das actualizações serem descarregadas mesmo que saia do Centro de Segurança.

- **Avisar antes de instalar actualizações** - cada vez que uma actualização for descarregada, será consultado antes da sua instalação ser feita.

Nota
Será avisado antes das actualizações serem instaladas mesmo que saia do Centro de Segurança.

13.2.3. Configurar Actualização Manual

Para definir como a actualização manual (actualização a pedido do utilizador) deve ser executada, seleccione uma das seguintes opções na categoria **Configuração Actualização Manual**:

- **Actualização silenciosa** - a actualização manual será feita em segundo plano automaticamente.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.

Nota
Será avisado antes das actualizações serem descarregadas mesmo que saia do Centro de Segurança.

13.2.4. Configuração Avançada

Para evitar que o processo de actualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar pelo reiniciar, em vez de o solicitar** - Se uma actualização requer um reiniciar, o produto continuará a funcionar com os antigos ficheiros até que o sistema reinicie. Ao utilizador não lhe será solicitado que o reinicie, logo o processo de actualização do BitDefender não interferirá com o trabalho do utilizador.

- **Não actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.

  Nota
  Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será cancelado.

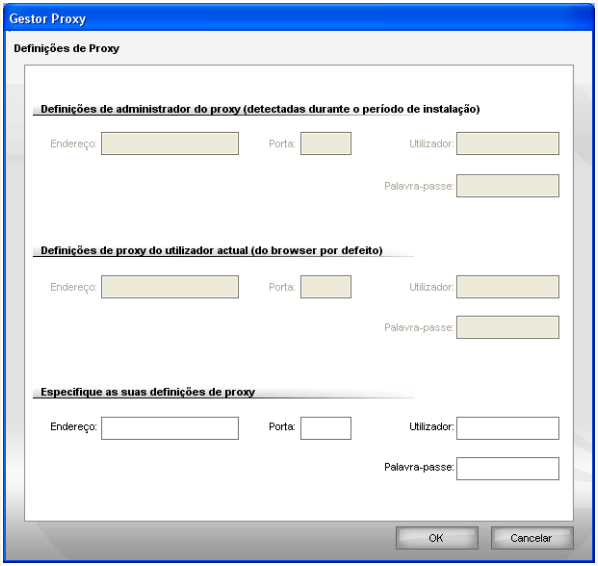
- **Não actualizar se o modo de jogo estiver ligado** - O BitDefender não actualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

13.2.5. Gerir Proxies

Se a sua empresa usa um servdior proxy para se ligar à Internet, deverá especificar as definições do proxy de forma a que o BitDefender se actualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o utilizador actual por defeito do browser, caso haja algum.

Nota
As definições do proxy só podem ser configuradas por utilizadores com direitos administrativos no computador ou por power users (utilizadores que sabem a palavra-passe da configuração do produto).

para gerir as definições do proxy, clique em **Gerir proxies**. A janela **Gsetor Proxy** irá aparecer.



Gestor Proxy

Existem três categorias de definições de proxy:

- **Definições de proxy de administrador (detectados durante o período de instalação)** - as definições de proxy detectadas da conta de administrador durante a instalação e que podem ser configuradas apenas se estive logged com essa conta. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.
- **Definições de proxy do utilizador actual (do browser por defeito)** - as definições de proxy do utilizador actual, extraidas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

Nota

Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se utiliza outro explorador por defeito, o BitDefender não será capaz de obter as definições do proxy do actual utilizador.

- **O seu próprio conjunto de definições de proxy** - definições de proxy que pode configurar se estiver logged in como administrador.

  As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
  - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

Quando tentar ligar-se à Internet, cada conjunto de definições do proxy é experimentado na sua vez, até que o BitDefender se consiga ligar.

Primeiro, o conjunto que contém as suas definições do proxy será utilizado para ligar a Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do utilizador actual serã retiradas do seu browser por defeito e usadas para obter a ligação à Internet.

Clique em **OK** para guardar as alterações e fechar a janela.

Clique em **Aplicar** para guardar as alterações, ou clique em **Por Defeito** para retornar às definições por defeito.

Administração de Backup Avançada

14. Administração de Backup Avançada

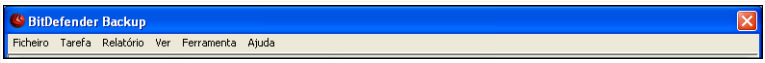
Neste capítulo ser-lhe-á dada uma introdução detalhada às características do interface gráfico do Backup Bitdefender.

Para dar início à configuração da definições de backup, apenas clique na barra **Backup** da área **Tarefas Rápidas** e depois clique em **Configuração Avançada**.

Existem duas formas como pode estabelecer e executar operações de backup. Ou acede à **Barra de Menu** superior, ou clica numa determinada barra a partir da **Barra de Navegação**.

14.1. Barra de Menu

Existem seis menus que pode usar para executar todas as funções oferecidas pela solução de backup BitDefender.



Barra de Menu

Ficheiro

- **Criar Nova tarefa:** Mostra uma caixa de diálogo de forma a criar uma nova tarefa de backup ou outra tarefa.
- **Abrir o Backup Set:** - Mostra uma caixa de diálogo de forma a abrir o backup set ou o catalog set para restauro.
- **Sair:** Permite sair da secção de backup BitDefender.

Tarefa

- **Backup:** Executa o backup de uma tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Restaurar Ficheiro:** Restaura a tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas .
- **Restaurar Dados em Ponto-Tempo:** Restaura a tarefa seleccionada para um determinado ponto do tempo. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Agendar:** Cria a tarefa agendada ou modifica a que já existe.
- **Apagar Agendar:** - Elimina o agendamento da tarefa agendada.
- **Apagar:** - elimina a tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.

- **Apagar Todas** - Elimina todas as tarefas no gestor de tarefas.
- **Explorar Destino:** Permite ver os dados do backup do destino da tarefa seleccionada.
- **Modificar Opções:** Modifica opções das tarefas seleccionadas.
- **Propriedades:** - PErmite modificar as propriedades de uma tarefa seleccionada, incluindo a fonte dos dados, nome, destino, etc, da tarefa.

Relatório

- **Ver Relatório:** Se a tarefa seleccionada contém definições de segurança, esta opção permite ver os conteúdos do relatório da tarefa.
- **Guardar como:** Guarda o conteúdo do relatório seleccionado para um determinado ficheiro.
- **Imprimir:** Imprime o conteúdo do relatório seleccionado.
- **Apagar Tudo:** - Apaga o conteúdo do relatório da tarefa seleccionada.
- **Actualizar:** Actualiza o conteúdo do relatório da tarefa seleccionada.

Ver

- **Introdução:** Se a janela da introdução não estiver a ser mostrada, esta opção permite abri-la.
- **Gestor de Tarefa:** Se a janela do gestor de tarefa não estiver a ser mostrada, esta opção permite abri-la.
- **Ver Log:** Se a janela do visualizador de logs não estiver a ser mostrada, esta opção permite abri-la.
- **Toolbox:** Se a janela não estiver a ser mostrada, esta opção permite abri-la.
- **Mostrar Barra de Menu:** Esconde a Barra de Menu. Para a mostrar, apenas prima **ALT**.
- **Mostrar Linha de Grelha:** Mostra ou esconde a linha de grelha. Aplica-se ao visualizador de logs e ao gestor de tarefas windows.

Ferramenta

- **Assistente de Backup:** Inicia o assistente de backup.
- **Assistente de Restauro** - Inicia o assistente de restauro.
- **Gravar:** Inicia a ferramenta de gravação de CD/DVD/ISO ou a ferramenta de gestão da gravação.
  - **Gravar CD/DVD**
  - **Gravar Ficheiros ISO**
  - **Ver Info Gravador**
- **Exportar todas Tarefas:** Exporta todas as tarefas criadas para um ficheiro específico.
- **Importar Tarefas:** Importa tarefas de um ficheiro `.JOB`, um ficheiro `.TXT` , ou um ficheiro `.XML`.
- **Exportar Logs:** Exporta logs para um ficheiro `.TXT` ou um ficheiro `.XML` .

- Para um ficheiro TXT
- Para um ficheiro XML

■ **Importar Logs:** Importa logs de um ficheiro .TXT ou de um ficheiro .XML .
- De um ficheiro TXT
- De um ficheiro XML

■ **Opções:** Modifica as suas opções gerais de backup.
- **Geral**
- **Relatórios & Log**
- **Agendar Tarefa**

Ajuda

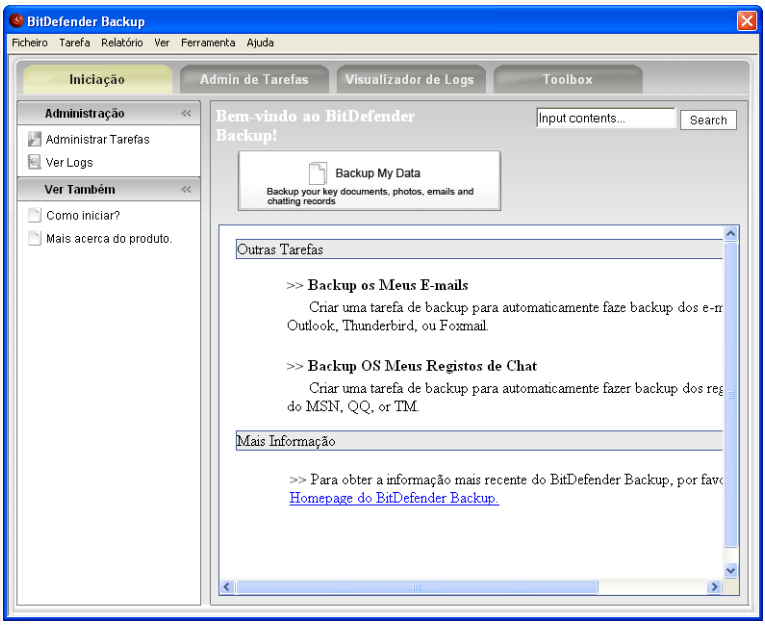
■ **Tópico de Ajuda:** Mostra tópicos de ajuda.
■ **Procurar:** Permite procurar tópicos de ajuda baseado nas palavras chave inseridas ou seleccionadas.
■ **BitDefender no Website:** Permite aceder à página da Internet do BitDefender e aceder às notícias BitDefender e ao suporte online.
■ **Acerca do Backup BitDefender :** Mostra o copyright, versão, e edição da info relacionada com o Backup BitDefender .

14.2. Barra de Navegação

A **Barra de Navegação**, mostrada na parte superior da janela principal e por debaixo da **Barra de Menu**, dá acesso a quatro secções:

■ **Introdução**
■ **Gestor Tarefas**
■ **Visualizador Log**
■ **Toolbox**

14.2.1. Introdução


BitDefender Backup
Ficheiro Tarefa Relatório Ver Ferramenta Ajuda
Iniciação
Admin de Tarefas
Visualizador de Logs
Toolbox
Administração
Administrar Tarefas
Ver Logs
Ver Também
Como iniciar?
Mais acerca do produto.
Bem-vindo ao BitDefender Backup!
Input contents...
Search
Backup My Data
Backup your key documents, photos, emails and chatting records
Outras Tarefas
>> Backup os Meus E-mails
Criar uma tarefa de backup para automaticamente faze backup dos e-m
Outlook, Thunderbird, ou Foxmail.
>> Backup OS Meus Registos de Chat
Criar uma tarefa de backup para automaticamente fazer backup dos reg
do MSN, QQ, or TM.
Mais Informação
>> Para obter a informação mais recente do BitDefender Backup, por favo
Homepage do BitDefender Backup.

Introdução

Pode mudar para a **Introdução** fazendo o seguinte:

- Clique em **Introdução** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Introdução**.
- Use um atalho premindo as teclas **CTRL+Alt+S**.

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão **Fazer Backup Dados** e siga o procedimento de três passos.

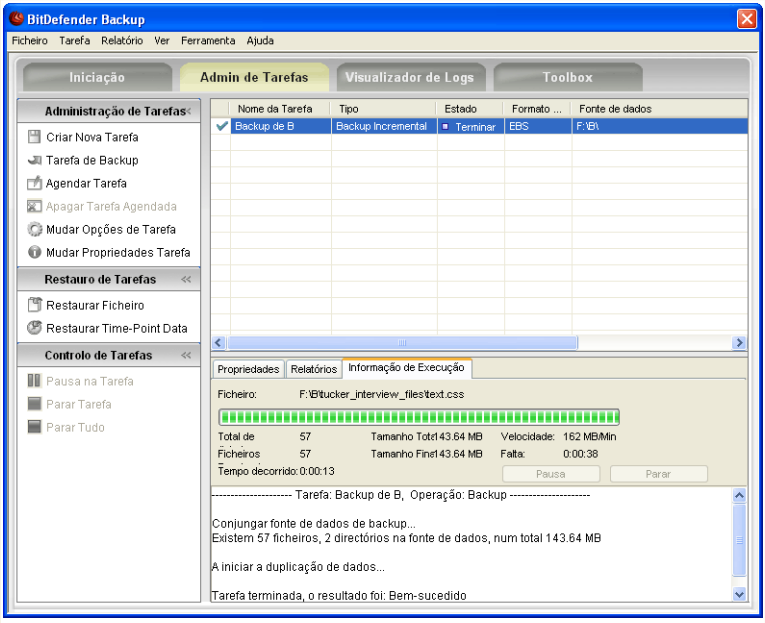
Para fazer backup apenas dos seus e-mails clique no botão **Fazer Backup E-mails** e siga o procedimento de três passos.

Para fazer backup apenas dos seus registos de chat, clique no botão **Fazer Backup do Chat** e siga o procedimento de três passos.

Nota
O procedimento de três passos é também descrito na secção Criar Nova Tarefa .

14.2.2. Gestor de Tarefa

Gestor de Tarefa é usado para ver e gerir tarefas de backup, ver proprieddes das tarefas e os relatórios das tarefas como também monitorizar a velocidade de execução da mesma. **Gestor de Tarefa** permite verificar as propriedades da tarefa e o seu estado actual, modificando as definições da tarefas como também executando a tarefa de backup ou restauro.



Gestor de Tarefa

Pode mudar para o **Gestor de Tarefa** fazendo o seguinte:

- Clique em **Gestor de Tarefa** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Gestor de Tarefa**.
- Use um atalho premindo as teclas **CTRL+Alt+M**.

À esquerda, poderá ver uma lista de links de operações rápidas, como se seguem:

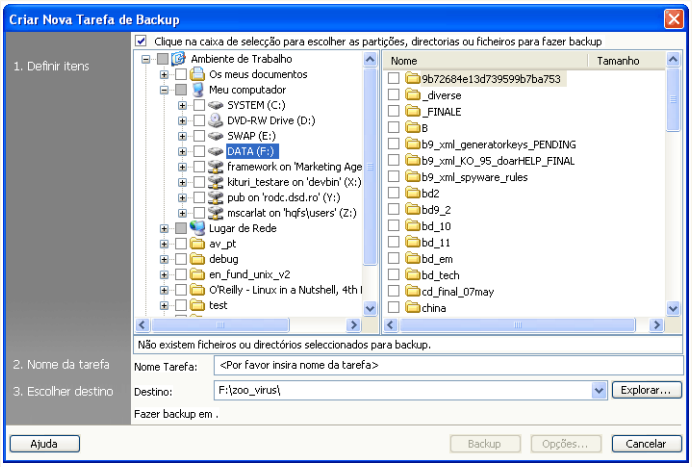
Gestão de Tarefa
- **Criar Nova Tarefa**
- **Tarefa de Backup**
- **Tarefa Agendada**
- **Apagar Tarefa Agendada**
- **Modificar Opções de Tarefa**
- **Modificar Propriedades de Tarefa**

Restaurar Tarefa
- **Restaurar Ficheiro**
- **Restaurar Dados Ponto-Tempo**

Controlo Tarefa
- **Pausa na Tarefa**
- **Parar Tarefa**
- **Parar Todas**

Criar Nova Tarefa

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão**Criar Nova Tarefa** e siga os próximos três passos.



Criar Nova Tarefa

1. Clique na caixa de selecção para selecionar partições, directórios, ou ficheiros para backup.

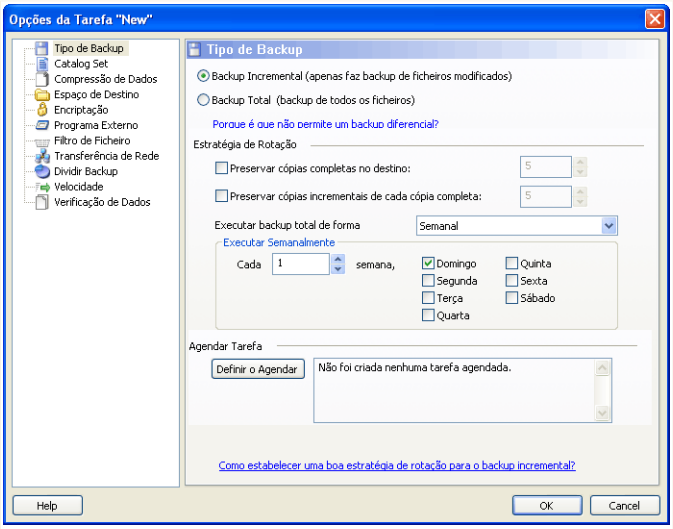
   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

   O nome por defeito da tarefa é automaticamente gerado quando os ficheiros ou os directórios são seleccionados para serem backup, mas pode ser modificado.
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Backup

Existem diversas sub-opções na caixa de diálogo das **Opções**.



Caixa de Diálogo Opções de Backup

Tipo de Backup

O Backup BitDefender suporta dois tipos de backup.

- **Backup Total:** Faz um backup completo de fonte de dados seleccionada para o backup set no destino especificado. Quando executar um backup total, o Backup BitDefender não fará backup dos dados modificados mas sim de toda a fonte de dados.
- **Backup Incremental:** Quando executar pela primeira o Backup Incremental é o mesmo que o Backup Total porque faz um backup completo de toda a fonte de dados para o backup set no destino especificado. Mais tarde, apenas faz backup dos novos ficheiros ou dos ficheiros modificados. Sempre que um Backup Incremental Backup é executado um backup catalog set é criado.

O Backup Incremental e o Total podem também combinar-se num **Backup de Rotação**. Por exemplo, pode definir um Backup Incremental do trabalho enquanto definie um Backup Total uma vez por semana, digamos ao Domingo. Eis como é feito: Seleccione **Semanal** do menu drop-down, `1` do campo**Cada Semana** e seleccionar Domingo. Este Backup Total ao Domingo substituirá todos os backups anteriores e será a base para o novo Backup Incremental trabalhar.

Catalog Set

É usado para indexar toda a informação de ficheiros de cada backup, e é a base do processos de Backup Incremental e Restauração. O catalog set (`*.ecs`) contém uma série de catálogos que representam um índice de todos os ficheiros e directórios existente no backup set. Tal índice inclui os dados da data do backup, directório de backup, nome do ficheiro e propriedades. Os dados podem ser restaurados a partir do catalog set.

Um nome de ficheiro de catalog set é gerado automaticamente por destino de tarefa. Para modificar o catalog set de uma tarefa faça o seguinte:

1. Clique em **Catalog Set**.
2. Insira um nome de ficheiro no campo correspondente.
3. Clique em **Explorar** para seleccionar o directório onde guardar os ficheiros do Catalog set.
4. Clique em **OK**.

Compressão de Dados

O Backup BitDefender permite a comprimir e guardar os dados para o backup set quando executa um backup para poupar espaço. Suporta Compressão Rápida, Compressão Standard, Compressão Alta Intensidade. Por exemplo, para iniciar a compressão standard a uma velocidade de compressão média, siga os seguintes passos:

1. Clique em **Compressão de Dados**.

2. Clique em **Compressão Standard**.
3. Clique em **OK**.

Span de Destino

O Backup BitDefender permite a distribuição do backup set para um destino diferente. neste caso, mesmo que um determinado destino não tenha suficiente espaço livre, a execução do backup dos dados prosseguirá.

Pode adicionar um ou mais destinos para continuar o backup, modificá-lo ou mesmo removê-lo, da seguinte forma:

1. Clique em **Span de Destino**.
2. Clique em **Adicionar** para seleccionar um novo destino para guardar os dados de backup..
3. Clique em **Editar** para modificar o destino de backup seleccionado.
4. Clique em **Apagar** para apagar o destino de backup seleccionado.
5. Clique em **Apagar Todos** para apagar todos os destinos de backup.
6. Clique em **OK**.

Encriptação

O Backup BitDefender mantém os dados backup mais seguros ao encriptá-los antes de os guardar no backup set. As definições de segurança de uma tarefa inclui protecção por palavra-passe.

Para encriptar os dados antes do backup, siga estes passos:

1. Clique em **Encriptação**.
2. Seleccione um tipo de encriptação a partir do menu drop-down.
3. Insira a sua palavra-passe no campo correspondente.
4. Reinsira a sua palavra-passe no campo correspondente.
5. Clique em **OK**.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa** .

3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do utilizador actual** quando o backup terminar.
7. Clique em **OK**.

Nota
Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de Ficheiros

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir ficheiros específicos, tipos de ficheiros ou directórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de ficheiros especifoicados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de ficheiros nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas tipos de ficheiros seleccionados** ou **Excluir tipos de ficheiros seleccionados** .
4. Se necessário, insira outro tipo de ficheiro no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um ficheiro especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Ficheiro**.
3. Exclua ou inclua ficheiros específicos nos pop-ups das caixas de diálogo seleccionando as opções **Incluir apenas os ficheiros especificados por regra** ou **Excluir os ficheiros especificados** .
4. Clique em **Explorar** e seleccione o ficheiro. O caminho da localização do ficheiro será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir o respectivo ficheiro da sua localização, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Transferência de Rede

O Backup BitDefender permite fazer backup e restaurar dados partilhados em grupos de trabalho de rede minuciosamente. Se a rede não estiver acessível, tentará fazer backup dos dados de vez em quando. Para especificar com que frequência ou quantas vezes deseja tentar o backup, siga os seguintes passos:

1. Clique em **Transferência de Rede**.
2. Clique em **Quando falhar em ler ficheiros de rede devido a desconexão, tentar conectar de novo**.
3. Insira com que frequência deseja tentar de novo o backup dos dados (em segundos).
4. Insira quantas vezes deseja tentar de novo o backup dos dados.
5. Clique em **OK**.

Nota

Para evitar ser esmagado por informação de erros de rede, clique em **Não é gerado relatório de erro quando a rede não está disponível**.

Dividir Backup Set

O backup set gerado pode ser dividido emdiveros outros backup sets, de forma a que o backup possa ser executado normalmente mesmo quando o destino ou o sistema de ficheiros é limitado. O Backup BitDefender dá-lhe dois métodos de divisão: auto-divisão e divisão-definida.

As definições de divisão da tarefa de backup podem ser modificadas da seguinte forma:

1. Clique em **Dividir Backup Set**.
2. Seleccionar **Divisão Automática por Espaço no Destino**.
3. Ou seleccione **Especificar tamanho para dividir** e escolha o tamanho desejado no menu drop down.
4. Clique em **OK**.

Velocidade

O Backup BitDefender suporta três tipos de velocidade. Quanto maior a velocidade, mais CPU será ocupado.

A velocidade de Backup pode ser especificada seguindo estes passos.

1. Clique em **Velocidade**.
2. Seleccione velocidade**Rápida**, **Média** ou **Baixa** .
3. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Tarefa de Backup

Uma vez que a tarefa tenha sido criada, o backup é executado automaticamente. No entanto, pode entrar em **Gestor de Tarefa** para executar backup ao seleccionar a tarefa criada e clicar no menu **Tarefa de Backup** .

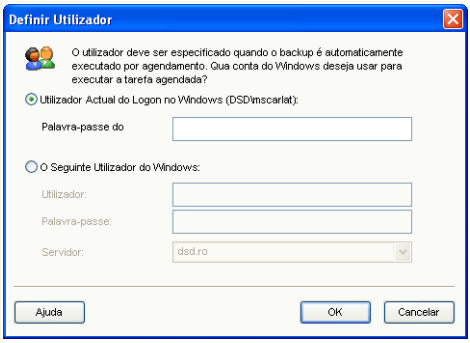
De forma a receber os detalhes do backup quando restaurar os ficheiros, deve de inserir uma breve descripção na janela de pop-up que se abre. Clique em **Cancelar** para ignorar a janela de pop-up ou **OK** para continuar. A tarefa de backup pode ser cancelada ao clicar no botão **Cancelar Backup** .

Nota

Para informação detalhada, uma boa ideia seria ver as **Propriedades**, **Relatórios** e **Info Execução** da tarefa a partir da janela da barra de estado.

Agendar Tarefa

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.



Agendar Tarefa

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Utilizador de Execução** aparecerá. Se é um utilizador do domínio, por favor insira a palavra-passe do domínio.
3. De outra forma seleccione **Executar como o seguinte utilizador Windows**.
4. Insira o nome do utilizador, palavra-passe e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o utilizador de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a tarefa agendada é executada (expresso como o número de dias ou semanas, o dia do mês ou a data). Outra

definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

    Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.
- **Tempo de Descanso**
  - Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

    Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
  - Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

    Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
  - Parar a tarefa se o computador deixar de estar em descanso.

    Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.
- **Gestor de Energia**
  - Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

    Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
  - Parar a tarefa se o modo de bateria iniciar.

    Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
  - Desperte o computador para executar esta tarefa.

    Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

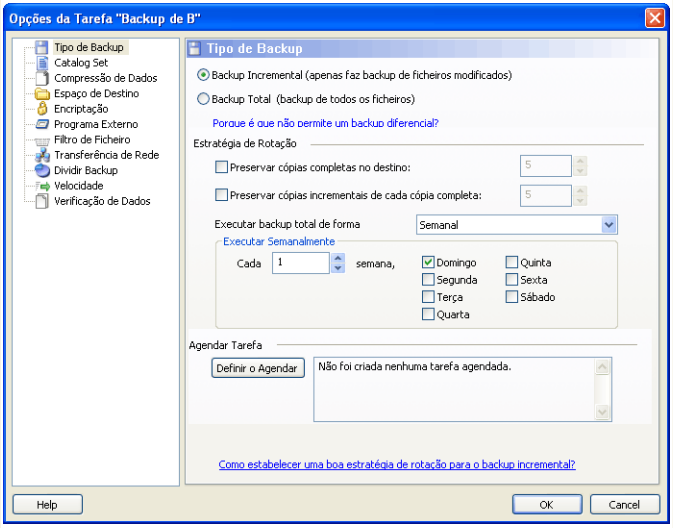
Apagar Tarefa Agendada

Para apagar uma tarefa agendada, seleccione-a e clique em**Apagar Tarefa Agendada** na secção**Gestão de Tarefas** .

Se a tarefa não está agendada, **Apagar Tarefa Agendada** será mostrada a cinzento, significando que não é usada.

Modificar Opções da Tarefa

Para modificar opções da tarefa, seleccione-a e clique em **Modificar Opções da Tarefa** na secção **Gestão de Tarefas** .

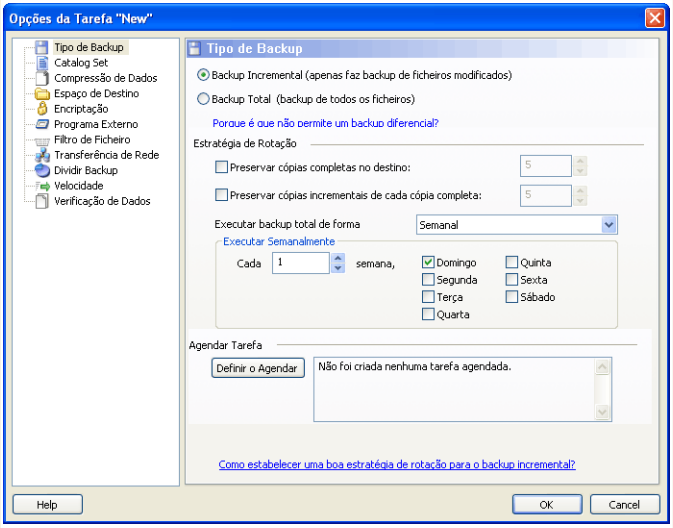


Modificar Opções da Tarefa

A tarefa seleccionada pode ser um backup ou uma gravação. Vamos pegar numa de cada vez.

Caixa de Diálogo Opções de Backup

Existem diversas sub-opções na caixa de diálogo das **Opções**.



Caixa de Diálogo Opções de Backup

Tipo de Backup

O Backup BitDefender suporta dois tipos de backup.

- **Backup Total:** Faz um backup completo de fonte de dados seleccionada para o backup set no destino especificado. Quando executar um backup total, o Backup BitDefender não fará backup dos dados modificados mas sim de toda a fonte de dados.
- **Backup Incremental:** Quando executar pela primeira o Backup Incremental é o mesmo que o Backup Total porque faz um backup completo de toda a fonte de dados para o backup set no destino especificado. Mais tarde, apenas faz backup dos novos ficheiros ou dos ficheiros modificados. Sempre que um Backup Incremental Backup é executado um backup catalog set é criado.

O Backup Incremental e o Total podem também combinar-se num **Backup de Rotação**. Por exemplo, pode definir um Backup Incremental do trabalho enquanto definie um Backup Total uma vez por semana, digamos ao Domingo. Eis como é feito: Seleccione **Semanal** do menu drop-down, 1 do campo**Cada Semana** e seleccionar Domingo. Este Backup Total ao Domingo substituirá todos os backups anteriores e será a base para o novo Backup Incremental trabalhar.

Catalog Set

É usado para indexar toda a informação de ficheiros de cada backup, e é a base do processos de Backup Incremental e Restauração. O catalog set (`*.ecs`) contém uma série de catálogos que representam um índice de todos os ficheiros e directórios existente no backup set. Tal índice inclui os dados da data do backup, directório de backup, nome do ficheiro e propriedades. Os dados podem ser restaurados a partir do catalog set.

Um nome de ficheiro de catalog set é gerado automaticamente por destino de tarefa. Para modificar o catalog set de uma tarefa faça o seguinte:

1. Clique em **Catalog Set**.
2. Insira um nome de ficheiro no campo correspondente.
3. Clique em **Explorar** para seleccionar o directório onde guardar os ficheiros do Catalog set.
4. Clique em **OK**.

Compressão de Dados

O Backup BitDefender permite a comprimir e guardar os dados para o backup set quando executa um backup para poupar espaço. Suporta Compressão Rápida, Compressão Standard, Compressão Alta Intensidade. Por exemplo, para iniciar a compressão standard a uma velocidade de compressão média, siga os seguintes passos:

1. Clique em **Compressão de Dados**.
2. Clique em **Compressão Standard**.
3. Clique em **OK**.

Span de Destino

O Backup BitDefender permite a distribuição do backup set para um destino diferente. neste caso, mesmo que um determinado destino não tenha suficiente espaço livre, a execução do backup dos dados prosseguirá.

Pode adicionar um ou mais destinos para continuar o backup, modificá-lo ou mesmo removê-lo, da seguinte forma:

1. Clique em **Span de Destino**.
2. Clique em **Adicionar** para seleccionar um novo destino para guardar os dados de backup..
3. Clique em **Editar** para modificar o destino de backup seleccionado.
4. Clique em **Apagar** para apagar o destino de backup seleccionado.
5. Clique em **Apagar Todos** para apagar todos os destinos de backup.
6. Clique em **OK**.

Encriptação

O Backup BitDefender mantém os dados backup mais seguros ao encriptá-los antes de os guardar no backup set. As definições de segurança de uma tarefa inclui protecção por palavra-passe.

Para encriptar os dados antes do backup, siga estes passos:

1. Clique em **Encriptação**.
2. Seleccione um tipo de encriptação a partir do menu drop-down.
3. Insira a sua palavra-passe no campo correspondente.
4. Reinsira a sua palavra-passe no campo correspondente.
5. Clique em **OK**.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do utilizador actual** quando o backup terminar.
7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de Ficheiros

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir ficheiros específicos, tipos de ficheiros ou directórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de ficheiros especifoicados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de ficheiros nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas tipos de ficheiros seleccionados** ou **Excluir tipos de ficheiros seleccionados** .
4. Se necessário, insira outro tipo de ficheiro no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um ficheiro especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Ficheiro**.
3. Exclua ou inclua ficheiros específicos nos pop-ups das caixas de diálogo seleccionando as opções **Incluir apenas os ficheiros especificados por regra** ou **Excluir os ficheiros especificados** .
4. Clique em **Explorar** e seleccione o ficheiro. O caminho da localização do ficheiro será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir o respectivo ficheiro da sua localização, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Transferência de Rede

O Backup BitDefender permite fazer backup e restaurar dados partilhados em grupos de trabalho de rede minuciosamente. Se a rede não estiver acessível, tentará fazer backup dos dados de vez em quando. Para especificar com que frequência ou quantas vezes deseja tentar o backup, siga os seguintes passos:

1. Clique em **Transferência de Rede**.
2. Clique em **Quando falhar em ler ficheiros de rede devido a desconexão, tentar conectar de novo**.
3. Insira com que frequência deseja tentar de novo o backup dos dados (em segundos).
4. Insira quantas vezes deseja tentar de novo o backup dos dados.
5. Clique em **OK**.

Nota

Para evitar ser esmagado por informação de erros de rede, clique em **Não é gerado relatório de erro quando a rede não está disponível**.

Dividir Backup Set

O backup set gerado pode ser dividido emdiveros outros backup sets, de forma a que o backup possa ser executado normalmente mesmo quando o destino ou o sistema de ficheiros é limitado. O Backup BitDefender dá-lhe dois métodos de divisão: auto-divisão e divisão-definida.

As definições de divisão da tarefa de backup podem ser modificadas da seguinte forma:

1. Clique em **Dividir Backup Set**.
2. Seleccionar **Divisão Automática por Espaço no Destino**.
3. Ou seleccione **Especificar tamanho para dividir** e escolha o tamanho desejado no menu drop down.
4. Clique em **OK**.

Velocidade

O Backup BitDefender suporta três tipos de velocidade. Quanto maior a velocidade, mais CPU será ocupado.

A velocidade de Backup pode ser especificada seguindo estes passos.

1. Clique em **Velocidade**.
2. Seleccione velocidade**Rápida**, **Média** ou **Baixa** .

3. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Modificar Opções da Tarefa de Gravação

Várias sub-opções estão disponíveis na caixa de diálogo da tarefa de gravação.

Gravar

Aqui é onde pode definir que o disco seja ejectado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o ficheiro de sistema Joliet (menos restrições no nome do ficheiro).

Se deseja agendar a tarefa, clique em **Definir Agendar**.

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Utilizador de Execução** aparecerá. Se é um utilizador do domínio, por favor insira a palavra-passe do domínio.
3. De outra forma seleccione **Executar como o seguinte utilizador Windows**.
4. Insira o nome do utilizador, palavra-passe e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o utilizador de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a

tarefa agendada é executada (expresso como o número de dias ou semanas, o dia do mês ou a data). Outra definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

    Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.
- **Tempo de Descanso**
  - Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

    Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
  - Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

    Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
  - Parar a tarefa se o computador deixar de estar em descanso.

    Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.
- **Gestor de Energia**
  - Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

    Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
  - Parar a tarefa se o modo de bateria iniciar.

    Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
  - Desperte o computador para executar esta tarefa.

Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:

1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do utilizador actual** quando o backup terminar.
7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de Ficheiros

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir ficheiros específicos, tipos de ficheiros ou directórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de ficheiros especifoicados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de ficheiros nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas tipos de ficheiros seleccionados** ou **Excluir tipos de ficheiros seleccionados** .
4. Se necessário, insira outro tipo de ficheiro no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando

inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um ficheiro especificado pode ser filtrado seguindo os seguintes passos:
1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Ficheiro**.
3. Exclua ou inclua ficheiros específicos nos pop-ups das caixas de diálogo seleccionando as opções **Incluir apenas os ficheiros especificados por regra** ou **Excluir os ficheiros especificados** .
4. Clique em **Explorar** e seleccione o ficheiro. O caminho da localização do ficheiro será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir o respectivo ficheiro da sua localização, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:
1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:
1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:
1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

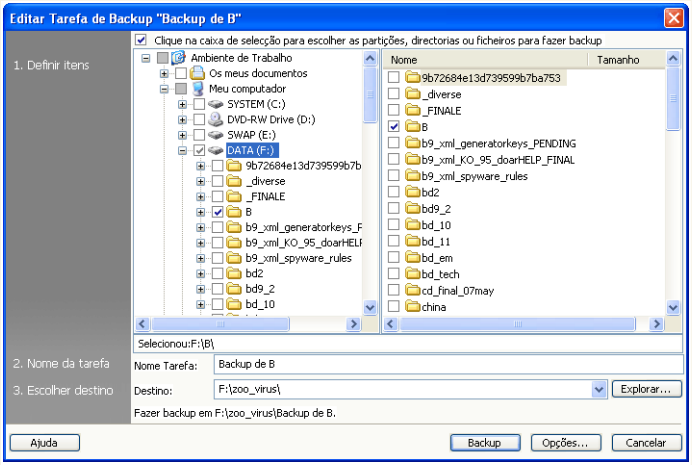
Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Modificar Propriedades da Tarefa

Para modificar as propriedades da tarefa, seleccione a tarefa em questão e depois clique em **Modificar Propriedades da Tarefa** na secção **Gestão de Tarefa**.



Modificar Propriedades da Tarefa

1. Clique na caixa de selecção para selecionar partições, directórios, ou ficheiros para backup.

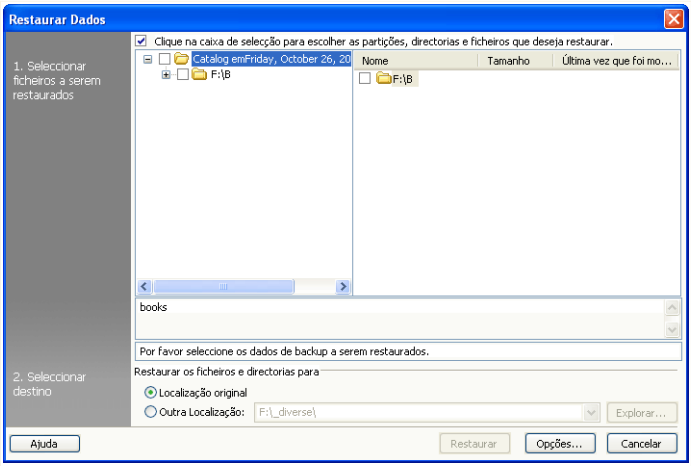
   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

   O nome por defeito da tarefa é automaticamente gerado quando os ficheiros ou os directórios são seleccionados para serem backup, mas pode ser modificado.
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Restaurar Ficheiro

Para restaurar o backup dos seus dados, seleccione a tarefa da qual deseja restaurar os dados, e clique em **Restaurar Ficheiro** no menu **Restaurar Tarefa** e depois siga estes passos.



Restaurar Ficheiro

1. Selecciones as caixas de selcção perto das partições, directórios, ou ficheiros seleccionados para serem restaurados.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo é mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Na janela **Seleccionar Local de Restauro**, pode usar o local original sem quaisquer mudanças, ou especificar outro local para onde restaurar o ficheiro.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar.

Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os ficheiros a serem restaurados já existem no destino na altura do restauro em si, e se actualiza a data modificada de cada ficheiro restaurado.

Quando os ficheiros a restaurar já existem

- **Ignorar Ficheiros** O BitDefender ignora os ficheiros respectivos.
- **Perguntar Utilizador** O BitDefender pergunta se deve ou não substituir os ficheiros existentes.
- **Substituir Directo** O BitDefender substitui os ficheiros sem perguntar.
- **Substituir Antigos** O BitDefender substitui apenas os ficheiros antigos. Os ficheiros antigos são determinados baseado na data em que foram modificados.

Data de Modificação do Ficheiro

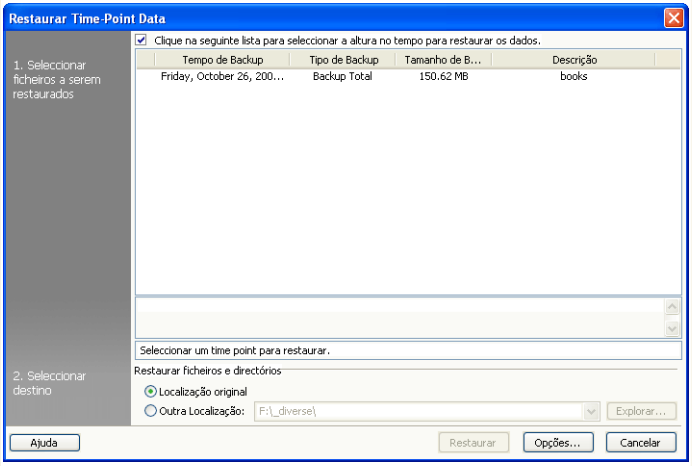
Se a opção for seleccionada, o BitDefender usa a data actual para indicar a data em que os ficheiros ou directórios foram restaurados. Se não, o BitDefender usa a data de modificação do ficheiro ou directório de quando eles foram backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Restaurar Dados do Ponto do Tempo

Para restaurar os dados de um backup de um determinado ponto do tempo, selecciona a tarefa da qual deseja restaurar os dados, e clique em **Restaurar Dados do Ponto do Tempo** no menu **Restaurar Tarefa** e então siga os seguintes passos.



Restaurar Dados do Ponto do Tempo

1. Seleccione o backup set de um determinado ponto do tempo da lista. Comentários serão mostrados por debaixo dele.
2. Na janela **Seleccionar Local de Restauro** , pode usar quer o local original, sem quaisquer alterações, ou especificar outro local para o qual restaurar o ficheiro.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os ficheiros a serem restaurados já existem no destino na altura do restauro em si, e se actualiza a data modificada de cada ficheiro restaurado.

Quando os ficheiros a restaurar já existem

- **Substituir Antigos** O BitDefender substitui apenas os ficheiros antigos. Os ficheiros antigos são determinados baseado na data em que foram modificados.

Data de Modificação do Ficheiro

Se a opção for seleccionada, o BitDefender usa a data actual para indicar a data em que os ficheiros ou directórios foram restaurados. Se não, o BitDefender usa a data de modificação do ficheiro ou directório de quando eles foram backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Controlo de Tarefa

Existem três formas de monitorizar uma tarefa: pausar a tarefa, parar a tarefa e parar todas.

Pausa

Para por em pausa um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Pausar Tarefa** no menu **Controlo de Tarefa** .

Parar

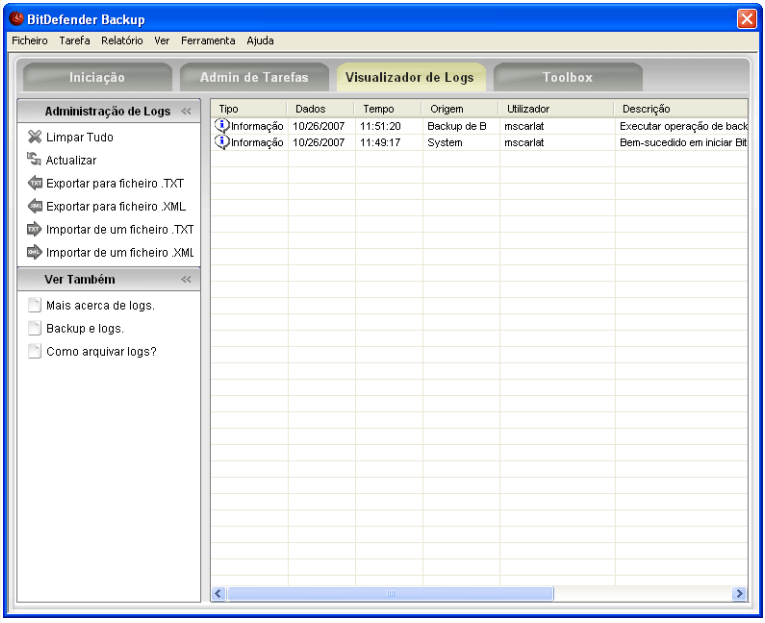
Para parar um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Parar Tarefa** no menu **Controlo de Tarefa** .

Parar Todas

Se existe mais do que uma tarefa de backup ou restauro a decorrer, não há necessidade de as parar uma a uma. Clique no botão **Parar Todas** no menu **Controlo de Tarefa** para as parar todas de uma só vez.

14.2.3. Visualizar Log

Esta secção mostra-lhe como ver, importar, exportar e limpar logs. A opção de Logs ajuda-o a lembrar do que fez backup ou restaurou e quando o fez e também mostra os avisos de erro das operações. Por exemplo, se um erro ocorreu quando um ficheiro foi lido durante a execução, o BitDefender regista-a como uma mensagem de aviso.



Visualizar Log

Pode mudar para **Visualizar Log** ao fazer uma das coisas seguintes:

- Clique em **Visualizar Log** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Visualizar Log**.
- Use um atalho ao premir as seguintes teclas **CTRL+Alt+L**.

Ver Logs

A opção de visualização de logs permite rastrear a sua operação, e descobrir a razão para a mesma ter falhado.

A descripção de um item de um log do Backup BitDefender contém os seguintes elementos:

Tipo

Uma classificação da severidade do item no log. Existem quatro graus de severidade no Backup BitDefender:

- **Fatal:** Um problema significativo que previne que o Backup BitDefender de decorrer normalmente. Por exemplo, o ficheiro de configuração do Backup BitDefender foi danificado.
- **Erro:** Um problema que leva a uma falha da operação. Por exemplo, uma tarefa que é backup num servidor, mas o servidor não pode ser acedido.
- **Aviso:** um problema que não afecta uma operação, mas que pode mais tarde ser classificado como um evento. Por exemplo, um ficheiro que não pode ser lido durante o backup.
- **Informação:** Descreve uma operação bem-sucedida. Por exemplo, uma tarefa foi apagada com sucesso.

Data
A data em que o item do log ocorreu.

Hora
A hora local em que o item do log ocorreu.

Fonte
A fonte que fez o log do respectivo item, que pode ser uma tarefa ou a aplicação do Backup BitDefender. Por exemplo, um item de sistema marcado indica que foi posto no log pela aplicação do Backup BitDefender. Outras possíveis marcas são os nomes das tarefas do Backup BitDefender terem feito log do respectivo item.

Utilizador
O nome do utilizador conforme com a acção do item que foi log.

Descripção
Apresenta o conteúdo detalhado do item que foi log.

Limpar Logs

O Backup BitDefender fornece duas formas de limpar logs: automaticamente e manualmente.

Importante
Uma vez que o registo de log tenha sido limpo, não pode mais ser recuperado. Logo é melhor exportar os logs para um ficheiro e preservá-los para futura consulta.

Limpar Automaticamente
Quando o Backup BitDefender inicia, compara o tamanho do log existente com o tamanho do log por defeito. O Backup BitDefender limpa automaticamente todos os ficheiros de log que excedam o tamanho por defeito.

Nota

Para saber mais ou modificar o tamanho por defeito do log siga os seguintes passos:

1. Clique em **Ferramenta** na **Barra de Menu**.
2. Clique em **Opções**, e depois seleccione **Relatórios & Log**.
3. Insira a desejada limitação de tamanho (em MB) no campo correspondente. Quando o ficheiro de log o atingir como limite, o Backup BitDefender limpará todos os logs.

Limpar Manualmente

Siga estes passos para limpar logs manualmente.

1. Clique em **Limpar Todos** no menu **Gestão de Logs** .
2. Clique em **OK** para exportar certos logs antes de limpar os outros, ou clique **Não** se não desejar preservar quaisquer logs.

Importar e Exportar Logs

O Backup BitDefender suporta actualmente importação e exportação de ficheiros em dois formatos: `.TXT` e `.XML`

Nota

Recomendamos que exporte e guarde o log para um ficheiro antes de o limpar.

Para exportar os logs para um ficheiro especificado, siga estes passos:

1. Clique em **Exportar para ficheiro .TXT** ou **Exportar para ficheiro .TXT** no menu **Gestão de Logs** .
2. Insira o nome do ficheiro e seleccione o local para onde guardar o ficheiro.
3. Clique em **Guardar**.

Para importar logs de um ficheiro específico, siga estes passos:

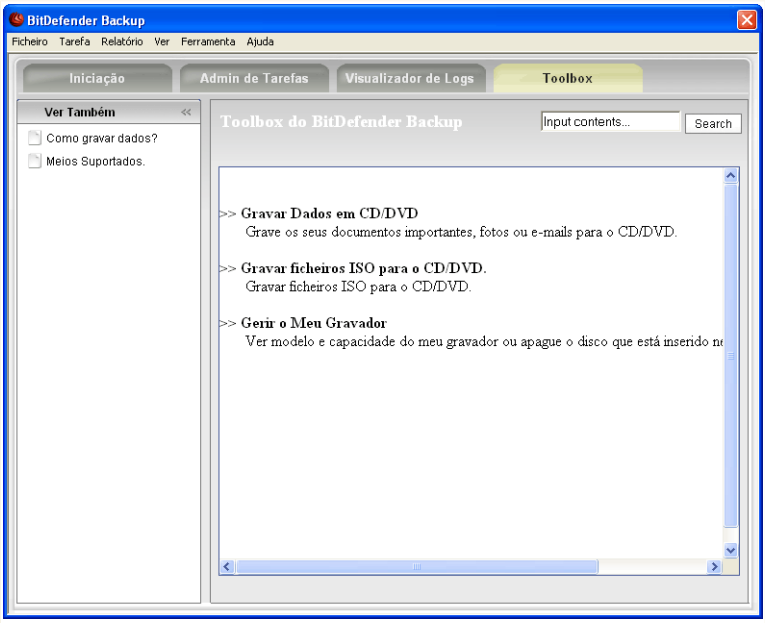
1. Clique em **Importar para ficheiro .TXT** ou **Importar para ficheiro .TXT** no menu **Gestão de Logs** .
2. Encontrar o seu ficheiro.
3. Clique em **Abrir**.

Nota

Clique no botão **Actualizar** no menu **Gestão de Logs** para ter a certeza que vê os logs mais recentes.

14.2.4. Toolbox

Esta secção mostra como usar o Backup BitDefender para gravar dados num CD/DVD ou para gravar um ficheiro de imagem ISO. Abrange assuntos tais como gravar um CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL e preservar dados em backup offline.


BitDefender Backup
Ficheiro Tarefa Relatório Ver Ferramenta Ajuda
Iniciação
Admin de Tarefas
Visualizador de Logs
Toolbox
Ver Também
Como gravar dados?
Meios Suportados.
Toolbox do BitDefender Backup
Input contents...
Search
>> Gravar Dados em CD/DVD
Grave os seus documentos importantes, fotos ou e-mails para o CD/DVD.
>> Gravar ficheiros ISO para o CD/DVD.
Gravar ficheiros ISO para o CD/DVD.
>> Gerir o Meu Gravador
Ver modelo e capacidade do meu gravador ou apague o disco que está inserido n

Toolbox

Pode mudar para **Toolbox** fazendo uma das coisas seguintes:

- Clique em **Toolbox** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Toolbox**.
- Use um atalho premindo as teclas **CTRL+Alt+T**.

Gravar para CD/DVD

Para gravar manualmente num CD/DVD, siga estes passos:

1. Clique em **Gravar dados no CD/DVD**.

2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   Aqui é onde pode definir que o disco seja ejectado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o ficheiro de sistema Joliet (menos restrições no nome do ficheiro).
4. Clique em **Ficheiro** ou **Directório** nos pop-ups da caixa de diálogo para adicionar dados que deseja gravar.
5. Após os dados terem sido adicionados, seleccione o gravador e insira o nome do disco onde vai gravar os dados, e depois clique em **Gravar**.

Gravar um ficheiro de imagem ISO para um CD/DVD

Para gravar um ficheiro de imagem ISO para um CD/DVD siga estes passos:

1. Clique em **Gravar um ficheiro de imagem ISO para um CD/DVD**.
2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   É aqui que pode definir ejectar o seu disco após gravação, finalizar o disco (se desja partilhá-lo com outros) ou escrever os dados usando o ficheiro de sistema Joliet (menos restrições de nome do ficheiro).
4. Clique em **Adicionar**.
5. Seleccione um ficheiro de imagem ISO para gravar e clique em **Abrir**.
6. Clique em **Gravar**.

Gerir o Meu Garvador

Isto ajuda-o a gerir e ver o dispositivo de gravação e de media do sistema actual. Contém os seguintes links:

- **Ejectar Dispositivo** Ejecta o dispositivo de gravação seleccionado.
- **Fechar Dispositivo** Fecha o dispositivo de gravação seleccionado.
- **Infos de Media** Permite visualizar a informação de Media do dispositivo de gravação.
- **Infos de Dispositivo** Permite visualizar a informação do dispositivo de gravação.
- **Capacidades** Permite visualizar as capacidades de gravação de media.
- **Apagar Media** Apaga o conteúdo do disco.

CD de Emergência BitDefender

15. Geral

O BitDefender Total Security 2008 vem num CD de arranque (Cd de Emergência BitDefender), capaz de analisar e desinfectar todos os discos duros antes do seu sistema operativo iniciar.

Deve usar o CD de Emergência BitDefender em qualquer altura que o seu sistema operativo não esteja a funcionar bem devido a infecções com vírus. Isso normalmente acontece quando não tem instalado um produto antivírus.

A actualização das assinaturas dos vírus é feita automaticamente, sem haver necessidade de intervenção por parte do utilizador, cada vez que arranca com o Cd de Emergência do BitDefender.

O CD de Emergência BitDefender é uma distribuição do Knoppix recompilada por BitDefender, que integra a mais recente solução BitDefender de segurança para Linux dentro do CD ao Vivo GNU/Linux Knoppix, que lhe oferece uma protecção instantânea de antivírus que é capaz de analisar e desinfectar discos duros existentes (incluindo partições Windows NTFS. Ao mesmo tempo, o CD de Emergência BitDefender pode ser usado para recuperar a sua preciosa informação quando não consegue arrancar com o Windows.

Nota
O Cd de Emergência do BitDefender pode ser descarregado deste link: http://download.bitdefender.com/rescue_cd/

15.1. Requisitos do Sistema

Antes de arrancar com o CD de Emergência BitDefender, deve em primeiro lugar verificar se o seu sistema possui os seguintes requisitos.

Tipo de Processador
x86 compatível, mínimo 166 MHz, mas não espere uma boa performance neste caso. A geração i686 de processador, a 800MHz, seria uma escolha mais apropriada.

Memória
Mínimo 512 MB de Memória RAM (1 GB recomendado)

CD-ROM
O CD de Emergência BitDefender, é executado a partir do CD-ROM, logo um CD-ROM e uma BIOS capaz de arrancar a partir do mesmo são necessários.

ligação Internet
Apesar de o CD de Emergência BitDefender se executar sem ligação à Internet, os processos de actualização requerem uma ligação HTTP activa, mesmo que seja através de um servidor proxy. Logo, para ter uma protecção actualizada, a Ligação à Internet tem de EXISTIR.

Resolução Gráfica
Placa gráfica Standard SVGA compatível.

15.2. Software incluído

O CD de Emergência BitDefender inclui os seguintes pacotes de software.

Xedit
Este é um ficheiro de um editor de texto.

Vim
Este é um poderoso ficheiro de um editor de texto, contendo uma sintaxe highlighting, uma GUI e muito mais. Para mais informação consulte a página web da Vim.

Xcalc
Este é uma calculadora.

RoxFiler
RoxFiler é um rápido e poderoso gestor de ficheiros gráficos.

Para mais informação, consultar a página internet da RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) um gestor de ficheiros em modo de texto.

Para mais informação, consultar apágina internet da MC.

Pstree
Pstree mostra processos que estão a decorrer.

Top
Top mostra as tarefas do Linux.

Xkill
Xkill mata um cliente com os seus recursos X.

Partition Image

Partition Image ajuda-o a guardar partições em ficheiros de sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 para um ficheiros de imagem. Este programa pode ser útil para propósitos de backup.

Para mais informação, consulte a página web da Partimage.

GtkRecover

GtkRecover é uma versão da GTK da recuperação do prgrama de consola. Ajuda-o a recuperar um ficheiro.

Para mais informação, consulte a página web da GtkRecover.

ChkRootKit

ChkRootKit é uma ferramenta que o ajuda a analisar o seu computador em busca de rootkits.

Para mais informação, consulte a página web do ChkRootKit.

Nessus Network Scanner

Nessus um analisador remoto de segurança para Linux, Solaris, FreeBSD, e Mac OS X.

Para mais informação, consulte a página web do Nessus.

Iptraf

Iptraf é um Software de Monitorização de Rede por IP.

Para mais informação, consulte a página web do Iptraf.

Iftop

Iftop mostra num interface o grau de utilização de banda.

Para mais informação, consulte a página web do Iftop.

MTR

MTR é uma ferramenta de diagnóstico de rede.

Para mais informação, consulte a página web da MTR.

PPPStatus

PPPStatus mostra as estatísticas acerca do tráfego TCP/IP de entrada e saída.

Para mais informação, consulte a página web da PPPStatus.

Wavemon

Wavemon uma aplicação de monitorização para dispositivos de redes wireless.

Para mais informação, consulte a página web da Wavemon.

USBView

USBView mostra informação acerca de dispositivos ligados ao USB bus.

Para mais informação, consulte a página web da USBView.

Pppconfig

Pppconfig ajuda-o a definir automaticamente uma ligação por dial up ppp.

DSL/PPPoe

DSL/PPPoe configura uma ligação PPPoE (ADSL).

I810rotate

I810rotate toggles o video output em i810 hardware usando o i810switch(1).

Para mais informação, consulte a página internet da I810rotate.

Mutt

Mutt é um poderoso cliente de e-mail MIME baseado em texto.

Para mais informação, consulte a página internet da Mutt.

Mozilla Firefox

Mozilla Firefox é um browser de internet bastante conhecido.

Para mais informação, consulte a página internet da Mozilla Firefox.

Elinks

Elinks um browser de internet em modo de texto.

Para mais informação, consulte a página internet da Elinks.

16. Como Usar o CD de Emergência BitDefender

Este capítulo comtém informação sobre como começar e parar o CD de Emergência BitDefender, analisar o seu computador em busca de malware como também guardar dadosdo seu comprometido PC Windows para um dispositivo amovível. No entanto ao usar as aplicações que vem com o CD, pode fazer muita tarefas cuja descripção vai muito para além deste manual de utilizador.

16.1. Iniciar o CD de Emergência BitDefender

Para iniciar o CD, prepare a BIOS do seu computador para arrancar pelo CD, coloque o CD na drive e reinicie o computador. Cerifique-se que o seu computador pode arrancar pelo CD.

Espere até ao próximo ecrã aparecer e siga as instruções no ecrã para iniciar o CD de Emergência BitDefender.

bitdefender
BitDefender Rescue CD
based on Knoppix
www.bitdefender.com
Press Enter to start or wait 30 seconds to boot from hard drive
F2 - Detailed options
BitDefender Rescue CD v2.0 http://www.bitdefender.com/
boot: _

Boot Splash Screen

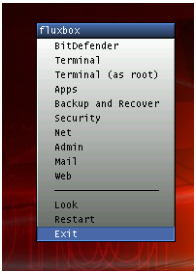
A actualização das assinaturas dos vírus é feita automaticamente, cada vez que arranca com o Cd de Emergência do BitDefender. Isto pode demorar um pouco.

Quando o processo de arranque terminar poderá ver o próximo ambiente de trabalho. Pode então começar a usar o CD de Emergência BitDefender.

O Ambiente de Trabalho

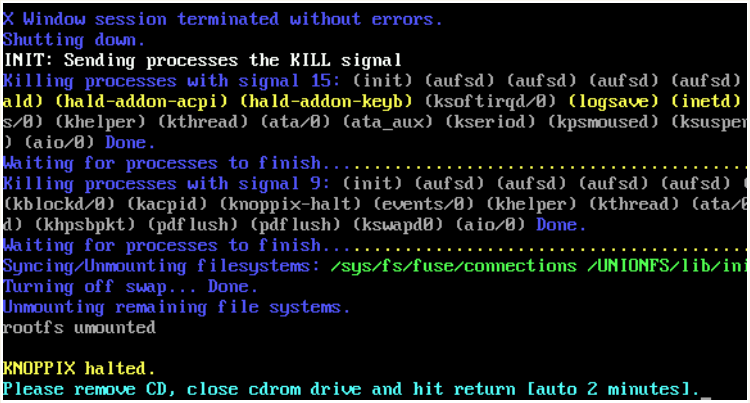
16.2. Parar o CD de Emergência BitDefender

Pode desligar em segurança o seu computador ao seleccionar **Sair** a partir do menu do CD de Emergência BitDefender (clique botão-direito para o abrir) ou ao emitir o comando **halt** num terminal.



Seleccionar "SAIR"

Quando o CD de Emergência BitDefender fechar com sucesso todos os programas mostra-lhe um ecrã como a imagem seguinte. Pode remover o CD de forma a arrancar pelo seu disco duro. Agora é OK desligar o seu computador ou reiniciá-lo.


X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].

Aguarde por esta mensagem quando estiver a desligar o seu pc

16.3. Como posso levar a cabo uma análise completa ao sistema?

Um assistente aparecerá quando o processo de arranque terminar e permite-lhe analisar totalmente o seu computador. Tudo o que tem de fazer é clicar no botão **Iniciar** .

Nota
Se a resolução do seu ecrã não for suficiente, ser-lhe-á solicitado que inicie a análise em modo de texto.

Siga o processo guiado de três passos para completar o processo de análise.

1. Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

2. Pode ver o número de incidências que afectam o seu sistema.

   As incidências são mostradas em grupos. Clique na caixa com o "+" para abrir um grupo, ou na caixa com o "-" para fechar um grupo.

   Pode escolher uma acção geral a ser tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.
3. Pode ver o resumo dos resultados.

Se deseja analisar uma determinada directoria apenas, faça o seguinte:

Explore as suas pastas, clique botão-direito num ficheiro ou directoria e seleccione **Enviar para**. Depois escolha **Analisador BitDefender**.

Ou pode emitir o próximo comando de raiz, de um terminal. O **Analisador Antivírus BitDefender** começará com o ficheiro ou pasta seleccionado como a localização por defeito a analisar.

```
# bdscan /path/to/scan/
```

16.4. Como posso actualizar o BitDefender através de um proxy?

Se existe um servidor proxy entre o vosso computador e a internet, algumas configurações têm de ser feitas de forma a poder actualizar o seu BitDefender.

Para actualizar o BitDefender através de um proxy, siga os seguintes passos:

1. Clique botão direito do rato sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Seleccione **Terminal (como raiz)**.
3. Digite o comando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Digite o comando: **mcedit bdscan.conf** para editar este ficheiro usando o GNU Midnight Commander (mc).
5. Uncomment a seguinte linha: `#HttpProxy =` (apenas apague o sinal `#`) e especifique o domínio, nome, palavra-passe e a porta do servidor proxy. Por exemplo, a linha respectiva deverá parecer-se com o seguinte:

```
HttpProxy = myuser:mypassword@proxy.company.com:8080
```

6. Prima **F2** para guardar o ficheiro actual, confirme o guardar, e depois prima **F10** para o fechar.
7. Digite o comando: **bdscan update**.

16.5. Como posso salvar os meus dados?

vamos partir do principio que não consegue arrancar o seu PC em Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente de aceder a alguma informação importante do seu computador. Eis aqui uma situação em que o CD de Emergência BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um stick de memória USB, siga os seguintes passos:

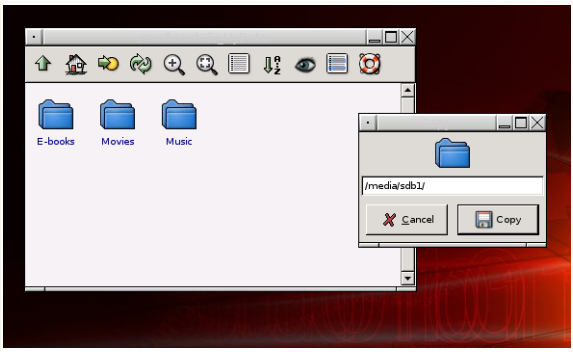
1. Coloque o CD de Emergência BitDefender na drive de CDs, e o stick de memória na entrada USB e depois reinicie o computador.
2. Espere que o CD de Emergência BitDefender termine de arrancar o PC. A seguinte janela irá aparecer.

Ecrã de Ambiente de Trabalho

3. Faça duplo clique sobre a partição onde os dados que deseja salvar se encontram (ex. `[sda3]`).

> **Nota**
> Quando está a trabalhar com o CD de Emergência BitDefender, estará a lidar com nomes de partições baseado em Linux. Assim, `[sda1]` provavelmente corresponderá à partição Windows `(C:)`, `[sda3]` a `(F:)`, e `[sdb1]` ao stick de memória.

4. Explore as suas pastas e abra a directoria que deseja. Por exemplo, `Meus Dados` que contém as sub-directorias`Filmes`, `Música` e `E-books` .
5. Clique botão direito do rato sobre a directoria desejada e seleccione **Copiar**. A seguinte janela irá aparecer:



Guardar Dados

6. Insira `/media/sdb1/` na correspondente caixa de texto e clique em **Copiar**.

Obter Ajuda

17. Suporte

Como um fornecedor importante, a BitDefender esforça-se por fornecer aos seus clientes um nível de suporte técnico sem igual de uma forma rápida e precisa. O Centro de Suporte (o qual poderá contactar nos endereços que lhe fornecemos abaixo) é continuamente mantido a par das mais recentes ameaças, e é aqui onde todas as suas questões são respondidas de uma forma rápida.

Com o BitDefender, tem sido sempre a nossa prioridade poupar aos nossos clientes tempo e dinheiro ao fornecer-lhes os produtos mais avançados aos preços mais económicos. Mais ainda, pensamos que um negócio de sucesso é baseado numa boa comunicação e num compromisso de excelência no suporte ao cliente.

Convidamo-lo desde já a colocar as suas questões em techsupport@bitdefender.pt a qualquer altura. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes que consiga acerca do seu BitDefender, acerca do seu sistema e uma descrição do problema tão completa e fiel quanto possível.

17.1. BitDefender Knowledge Base

A BitDefender Knowledge Base é um repositório de informação on-line acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das actividades de reparação de erros por parte da equipe técnica do suporte BitDefender e da equipe de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de vírus, a administração de soluções BitDefender e explicações pormenorizadas, e muitos outros artigos.

A BitDefender Knowledge Base encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na BitDefender Knowledge Base, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

A BitDefender Knowledge Base encontra-se disponível a qualquer altura em http://kb.bitdefender.com.

17.2. Pedir Ajuda

17.2.1. Vá até ao Self-Service Web

Tem uma dúvida? Os nossos peritos em segurança estão disponíveis para o ajudar 24/7 via e-mail ou chat sem custos adicionais.

Por favor siga os seguintes links:

English

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2193/

German

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2193/

French

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2193/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2193/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2193/

17.2.2. Abrir um ticket de suporte

Se deseja abrir um ticket de suporte e receber ajuda via e-mail, siga os seguintes links:

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

17.3. Informação de Contacto

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

17.3.1. Endereços Web

Departmento Comercial: comercial@bitdefender.pt
Suporte Técnico: support@bitdefender.com
Documentação: documentation@bitdefender.com
Partner Program: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Contactos Imprensa: pr@bitdefender.com
Oportunidades de Trabalho: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Site internacional do produto: http://www.bitdefender.com
Ficheiros ftp do produto: ftp://ftp.bitdefender.com/pub
Distribuidor Local: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

17.3.2. Escritórios

Os escritórios BitDefender estão preparados para responder a quaisquer perguntas respeitantes às suas áreas de operação, quer sejam questões comerciais e de assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Suporte Técnico:

- support@bitdefender.com

- Telefone:
  - 1-888-868-1873 (Registered Users Only; accessible in United States only)
  - 1-954-776-6262 (Registered Users Only)

Serviço ao Cliente:

- E-mail: customerservice@bitdefender.com
- Telefone:
  - 1-888-868-1873 (Registered Users Only; accessible in United States only)
  - 1-954-776-6262 (Registered Users Only)

Alemanha

BitDefender GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Alemanha
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
Email: info@bitdefender.com
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Suporte Técnico: support@bitdefender.com

UK e Irlanda

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: info@bitdefender.com
Sales: sales@bitdefender.com
Web: http://www.bitdefender.co.uk
Suporte Técnico: support@bitdefender.com

Espanha

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006

Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender.pt
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Suporte Técnico: support@bitdefender.com
Sales: sales@bitdefender.com
Phone: +40 21 4085600
Fax: +40 21 2330763
Site internacional do produto: http://www.bitdefender.com

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável por uma falta completa de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa das aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Arquivo

Um disco, cassete, ou directório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Backdoor

Um buraco na segurança de um sistema deliberadamente criado pelos desenhadores ou responsáveis da manutenção. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, que trazem contas privilegiadas, criadas para serem usadas pelos técnicos de serviço ou pelo vendedor dos programas de manutenção.

Sector de arranque

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí fora). Para discos de inicialização, o sector de saída também contém um programa que carrega o sistema operativo.

Vírus de boot

Um vírus que infecta o sector boot de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infectada por um vírus de boot, irá causar a activação do vírus em memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo em memória.

Browser

Diminuitivo para browser de internet, que é um software usado para localizar e mostrar páginas Web. Os dois mais populares browsers são o Netscape Navigator e o Microsoft Internet Explorer. Ambos são browsers gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos browsers modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de necessitarem de plug-ins para alguns formatos.

Linha de comando

Numa interface de linha do comado, o utilizador introduz comandos no espaço providenciado directamente no ecrã, usando a linguagem de comando.

Cookie

Dentro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Enquanto este ponto de vista possa ser extremo, em alguns casos é exacto.

drive de disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma drive de disco rígido lê e escreve nos discos rígidos.

Uma drive de disquetes acede às disquetes.

As drives dos discos tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Download (Descarga)

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. Também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

E-mail

Correio electrónico. É um serviço que envia mensagens em computadores via redes locais ou globais.

Eventos

Uma acção ou ocorrência detectada por um programa. Os eventos podem ser acções do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tal como ficar sem memória.

Falso positivo

Ocorre quando o analisador identifica um ficheiro como infectado, quando na verdade ele não está.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras. Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostEscrito, ".txt" para texto arbitrário.

Heurístico

Um método baseado na regra de identificar novos vírus. Este método de análise que não se baseia em assinaturas específicas de vírus. A vantagem da análise heurística, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP que é responsável dos endereços de IP, rotas, e a fragmentação e reassemblagem dos pacotes de IP.

Java applet

Um programa em Java desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o browser descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do qual elas são servidas.

Macro vírus

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Não-heurístico

Este método de análise depende da assinaturas de vírus especificas. A vantagem de uma análise não-heurística, é que ela não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente isto iria requerer dez de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número

de espaços a serem substituidos. Neste caso, os dez espaços iriam requerer apenas dois bytes. Esta é apenas uma técnica de compactar, há muitas.

Caminho

As direcções exactas para um ficheiro num computador. Estas direcções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dois quaisquer pontos, tal como os canais de comunicação entre dois computadores.

Phishing

O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoal, tal como palavras-passe e números de cartões de crédito, segurança social, e números de contas bancárias, que a legítima organização já possui. O site web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Vírus polimórfico

Um vírus que altera a sua forma com cada ficheiro que infecta. Dado que eles não têm uma padrão de patente binária consistente, tais vírus são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais têm vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e teclados. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto final para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ficheiro de relatório

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender mantém um ficheiro de relatório que lista o caminho analisado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar

nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detectados.

Script

Outro termo para macro ou batch file, um script é uma lista de comandos que podem ser executados sem a interacção do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

Spyware

O estabelecimento de ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo palavras-passe e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as

aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens no Startup

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Área de notificação

Introduzido com o Windows 95, a área de notificação está localizada na barra de tarefas do Windows (normalmente em baixo junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema tais como, fax, impressora, modem, volume, etc. Faça duplo-clique ou clique botão-direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho largamente usados na Internet e que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operativos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

Trojan

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais insidiosos é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Actualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O BitDefender tem o seu próprio módulo de actualização que lhe permite verificar actualizações manualmente, ou actualizar o produto automaticamente.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Um tipo de vírus ainda mais perigoso é aquele que é capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

assinatura de vírus

O padrão binário de um vírus, usado pelo programa antivírus para detectar e eliminar o vírus.

Worm

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.